RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CSV-W04

Security, Meet Your New Roommate, The Dynamic Provisioning Environment

Jason Pappalexis
Research Director
NSS Labs, Inc.
@jsnppp

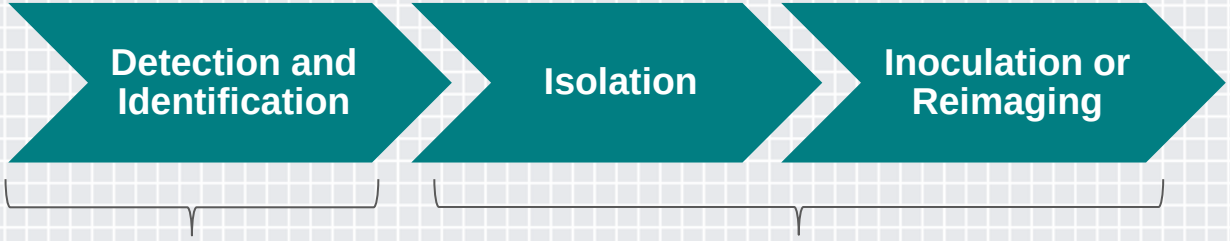
Chris Morales
Principal Engineer
HyTrust
@MoralesATX

Security Requires Flexibility

Adaptive

Resilient

Incident Response Still Includes Reimaging



Remediation through reimaging solves **business** need,

*not **security** need*

Forensics Enables Understanding

Forensics can add considerable time to remediation process

*with **no guarantee of successful results***

The Incident Response Conundrum

Reimaging	Forensics
Rapid Resolution	Time-consuming Resource-intensive
Threat Removal	Threat Retention (+ Possible Reinfection)
Intelligence Gathering *Small Amount*	Intelligence Gathering *Large Amount*
Business **Continuity**	Business **Impact**

If Only We Had...

Phantom Zone

RSAConference2015

San Francisco | April 20-24 | Moscone Center

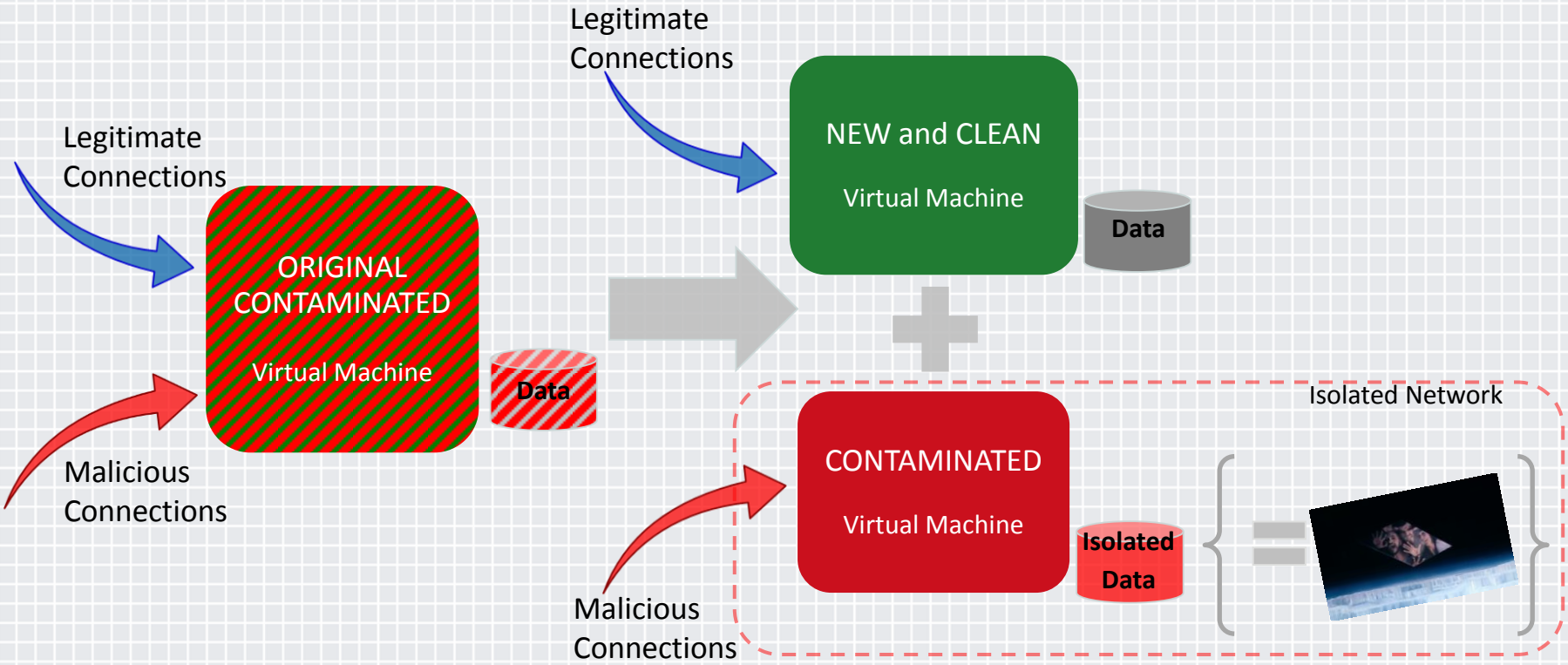
Virtualization Unlocks Doors

NSS LABS

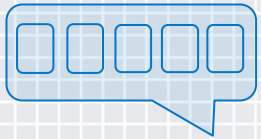
Most Enterprise Environments Are Virtualized

- Virtual data centers **are growing**
  - >**50%** of today's organizations have a virtual component
  - Top companies have **>30,000** virtual machines
  - Many have capacity **not being utilized**
- Dynamic provisioning environment (DPE)
  - Central management and provisioning of **virtual machines** (VMs)
  - **Rich APIs** provide options for control
  - Automation **saves time** and can **reduce error**

Duplication Of Work Surface Using DPE



How It Works – Five Phases Of Adaptive Security



EVALUATION	CLONING	TRANSFERENCE	CONTAINMENT	COMMUNICATION

This process is not owned by a single person today

How It Works – Evaluation

EVALUATION

- Processes
- Resources
- Services
- Connections

Unix *netstat* command

```
$ sudo netstat -lp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address   Foreign Address State    PID/Program Name
tcp        0      0 *:http-alt      *:*             LISTEN   6022/java
tcp        0      0 *:ssh           *:*             LISTEN   29126/sshd
tcp        0      0 *:8443          *:*             LISTEN   6022/java
tcp        0      0 *:1883          *:*             LISTEN   2237/mosquitto
udp        0      0 *:mdns          *:*                      6022/java
udp        0      0 localhost:ntp   *:*                      2260/ntpd
Active UNIX domain sockets (only servers)
Proto RefCnt Flags   Type      State      I-Node   PID/Program Path
unix  2      [ ACC ] SEQPACKET  LISTENING 3829     159/udevd /run/udev/control
```

VMware List Processes

```
VixVM_ListProcessesInGuest(VixHandle vmHandle,
                           int options,
                           VixEventProc *callbackProc,
                           void *clientData);
```

VMware VIX API v1.13 - https://www.vmware.com/support/developer/vix-api/index.html

How It Works – Cloning

CLONING

Duplicate VM without connections

Citrix XenServer

```
VM.clone(session, t_ref, ”VM_Name")
VM.provision(session, new_vm_ref)
```

VMware ESX

```
VixVM_Clone(VixHandle vmHandle,
            VixHandle snapshotHandle,
            VixCloneType cloneType,
            const char *destConfigPathName,
            VixCloneOptions options,
            VixHandle propertyListHandle,
            VixEventProc *callbackProc,
            void *clientData);
```

VMware VIX API v1.13 - https://www.vmware.com/support/developer/vix-api/index.html
Xen: http://docs.vmd.citrix.com/XenServer/6.0.0/1.0/en_gb/api/?c=VM

How It Works – Transference

TRANSFERENCE

Legitimate connections transparently moved to new clone

Unix *iptables* command

```
# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
```

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

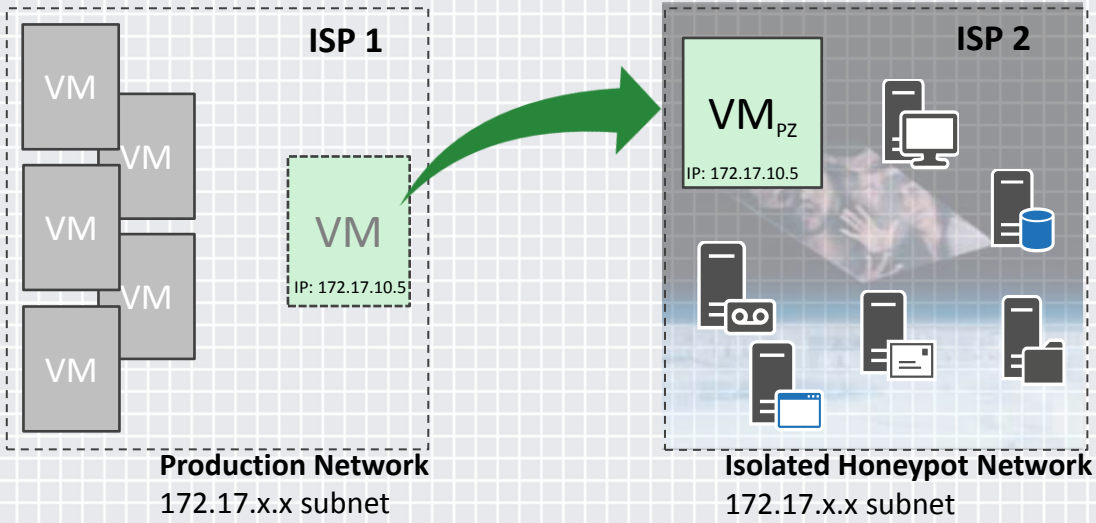
How It Works – **Containment**

VMware ESX

```
./esxcfg-portgroup-mgmt.pl
     --server esxi4-2.primp-industries.com
     --username root --operation enable
     --portgroup "Management Network"
     --portgroup_type vmotion
```

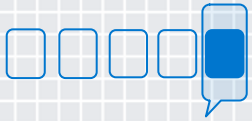
CONTAINMENT

Attacker's progress is preserved



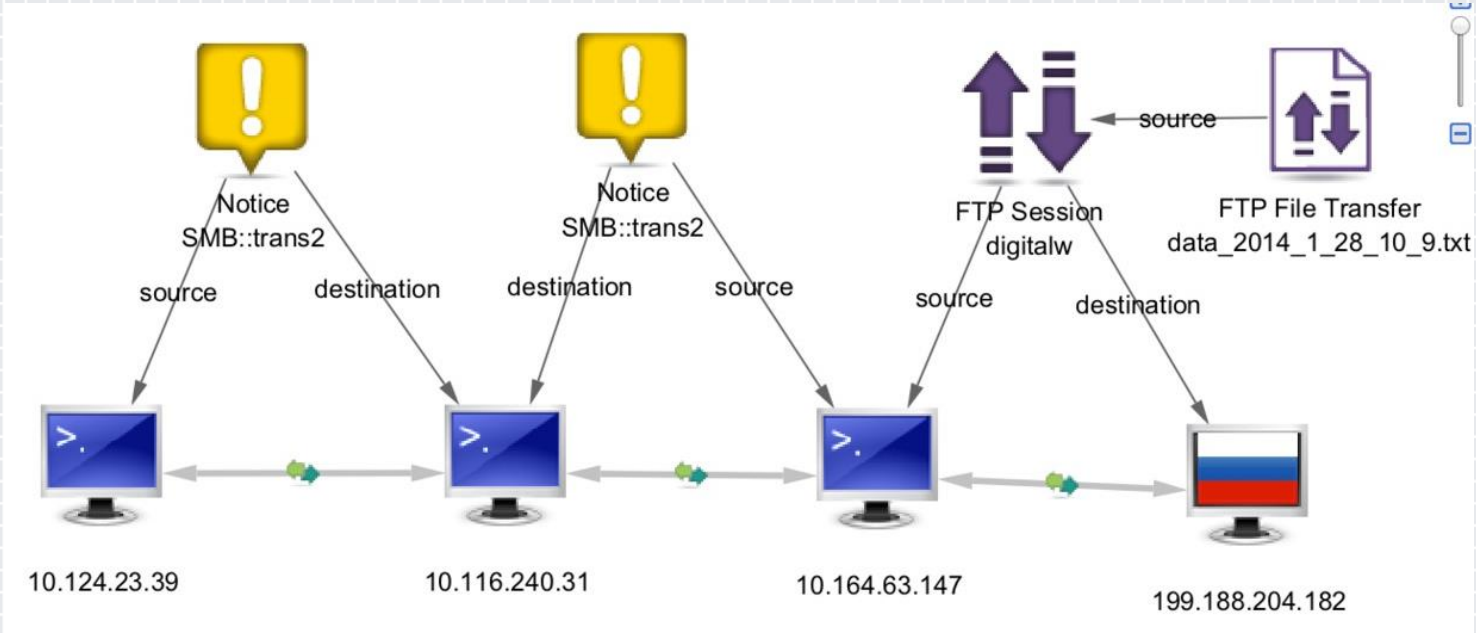
The contaminated VM is moved to secure, isolated, honeypot network

How It Works – **Communication**



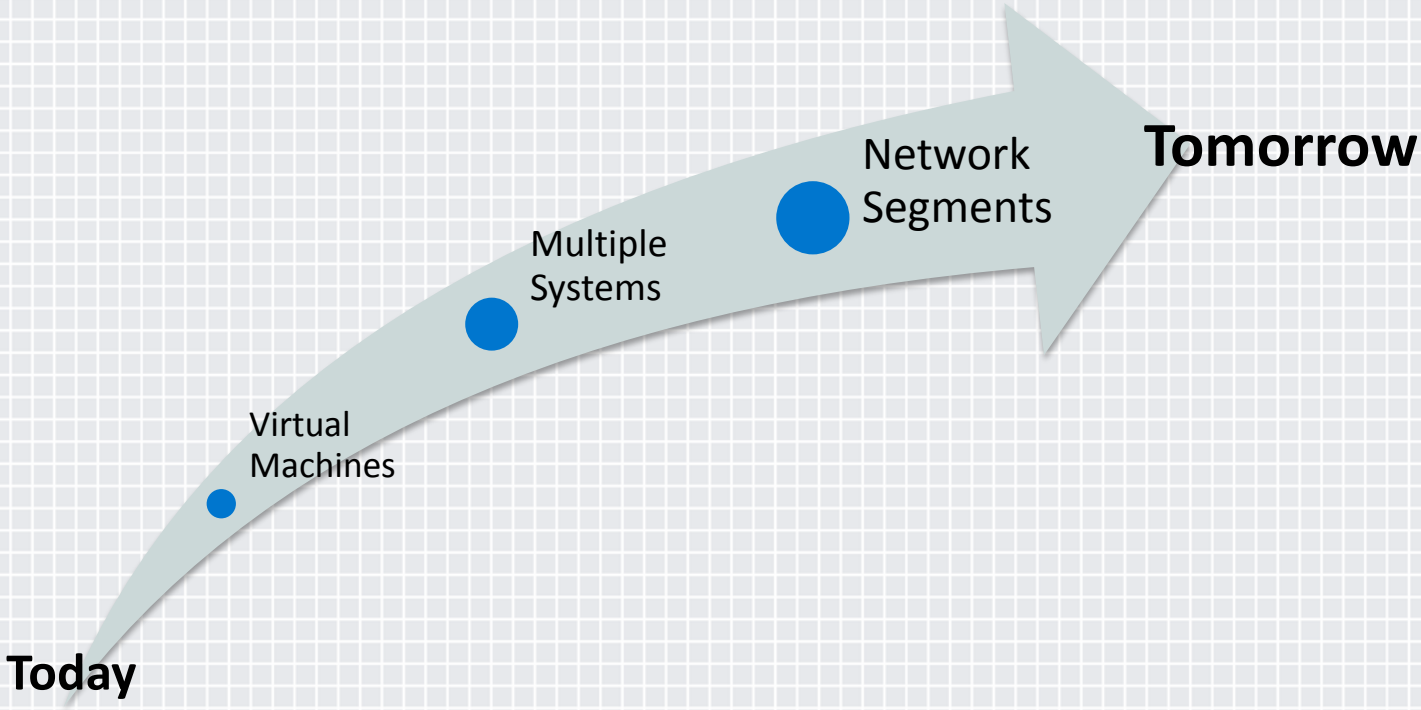
COMMUNICATE

Identify where the attack surface needs to adapt and then Implement



Source: 21CT LYNXeon Network Security Analytics

To Infinity And Beyond



Apply What You Have Learned Today

- *Next week* you should:
  - Confirm if your company detonates known bad infections
  - Investigate if re-imaging is the primary method of remediation
- *In the first three months* following this presentation you should:
  - Discuss resiliency of mission critical systems within your network
  - Review spare capacity in virtual data centers within your network
- *Within six months* you should:
  - Define a process and automation
  - Define success metrics – when is this a viable option for your company

Security Requires Flexibility

Adaptive

Resilient

References and Resources

- Cyber Resilience: It's Not About the 98 Percent You Catch, It's About the 2 Percent You Miss. NSS Labs, https://www.nsslabs.com/reports/cyber-resilience-it's-not-about-98-percent-you-catch-it's-about-2-percent-you-miss
- Adaptive Security for Business Continuity. NSS Labs, https://www.nsslabs.com/reports/adaptive-security-business-continuity-0
- Incident Response Part 1: Does It Matter, Or Was It Just Noise? NSS Labs, https://www.nsslabs.com/reports/incident-response-part-1-does-it-matter-or-was-it-just-noise
- Incident Response Part 2: Breach Found. Did it hurt? NSS Labs, https://www.nsslabs.com/reports/incident-response-part-2-breach-found-did-it-hurt

RSAConference2015

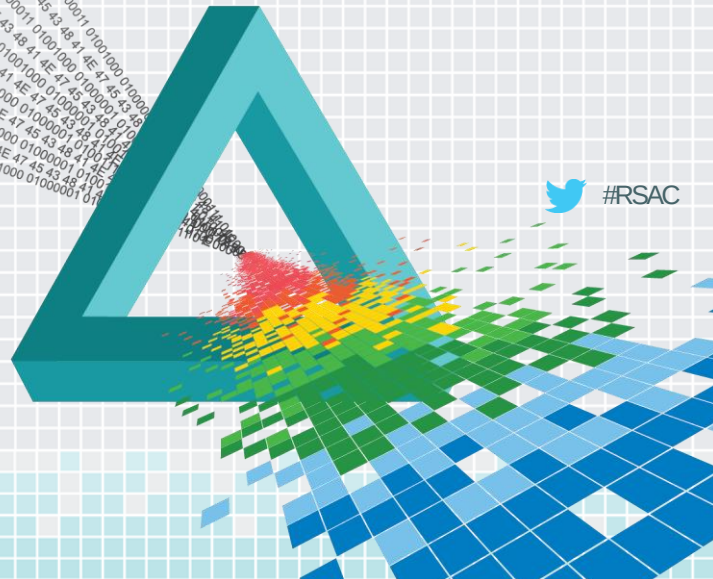
San Francisco | April 20-24 | Moscone Center

Thank you!

Jason Pappalexis
Research Director, NSS Labs, Inc.
jpappalexis@nsslabs.com

Chris Morales
Principle Engineer, HyTrust, Inc.
cmorales@hytrust.com

Questions and Answers



NSS LABS