NeuVector

Docker Hack

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

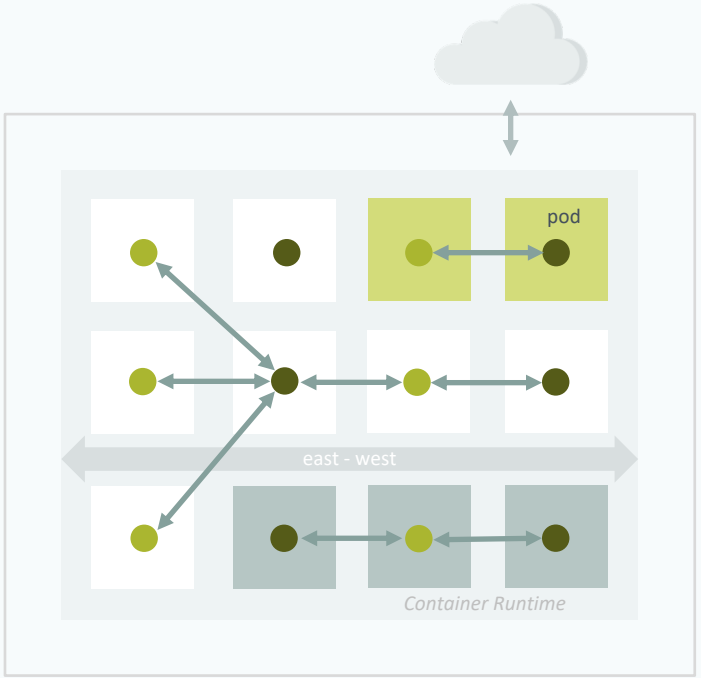
Dieter Reuter
Chief Solutions Architect, Docker Captain

@Quintus23M, dieter@neuvector.com

redhat. CERTIFIED TECHNOLOGY

docker CERTIFIED

Microservice Architecture: New Challenges and Risks



Container NODES

- Hyper Scale
- East-West Traffic Explosion
- Low Visibility
- Open Source Vulnerabilities
- Sophisticated Insider Attacks

- Multi-vector Detection
- Security Automation

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

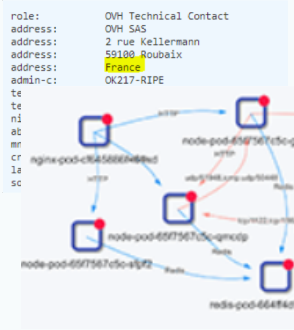
Hackers exploit Jenkins servers, make $3 million by mining Monero

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

Traditional Security - Blind!

Muhstik Botnet: In AWS Honeypot

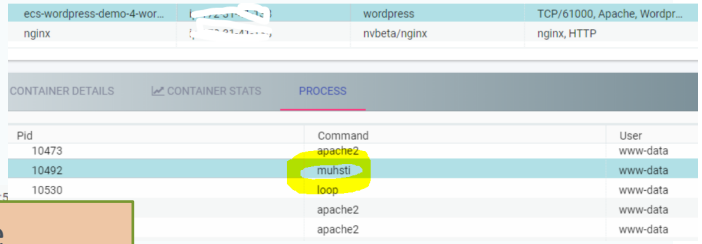
Discover Vulnerable Wordpress



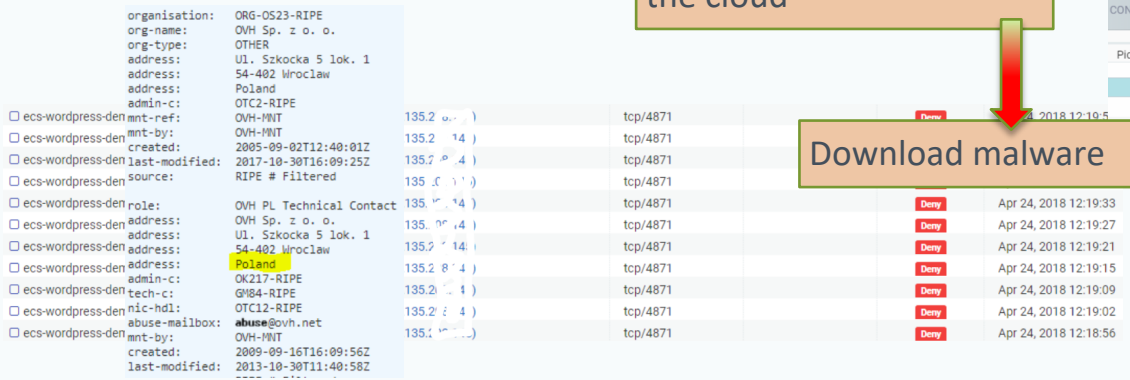
Exploit: Overwrite Wordpress theme PHP files

```
# cat muhstik.php
<?php eval(base64_decode('ZWNobyA
BpZD0idXBsb2FkZXIiPic7ZWNobyAnPG1uchV0InK5cGU
BPU1RbJ191cGwnXSA9PSAiVXBsb2FkIiApIHsgaWYoQGN
VjaG8gJzxiPlVwbG9hZCBGYWlsZWQuPC9iPjxicj48YnI
```

Connect to C&C server in the cloud

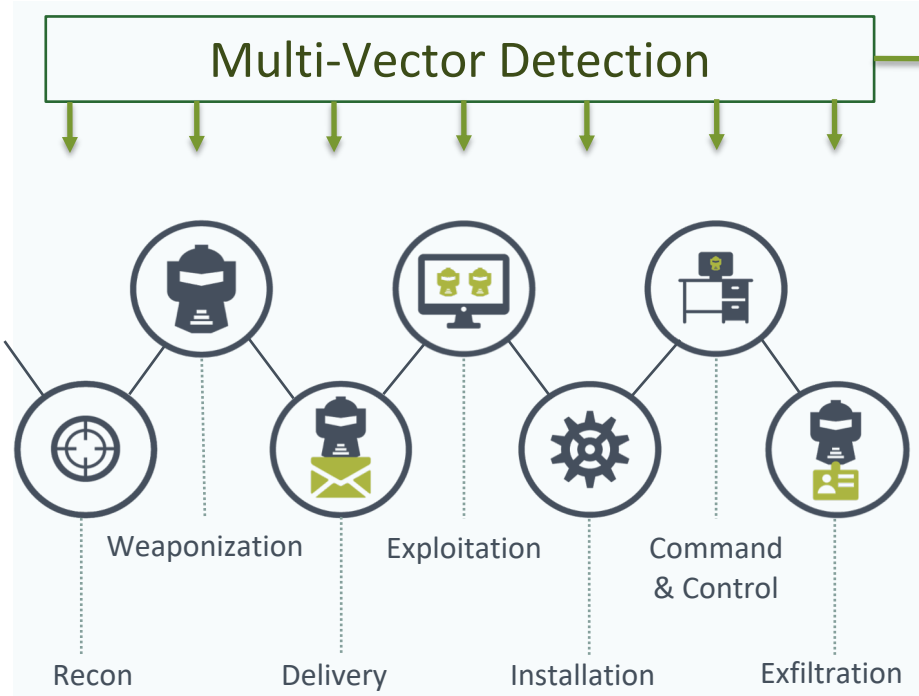


Download malware



Propagate and Initial DDoS attack

Detecting the Kill Chain Events – At Run-Time



	Network	Container	Host
Cryptojacking Bitcoin Mining	✓		✓
Port Scan	✓		
EQUIFAX DATA BREACH	✓	✓	
DDOS ATTACK	✓		
SQL	✓		
DIRTY COW		✓	✓
Apache Struts	✓	✓	

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

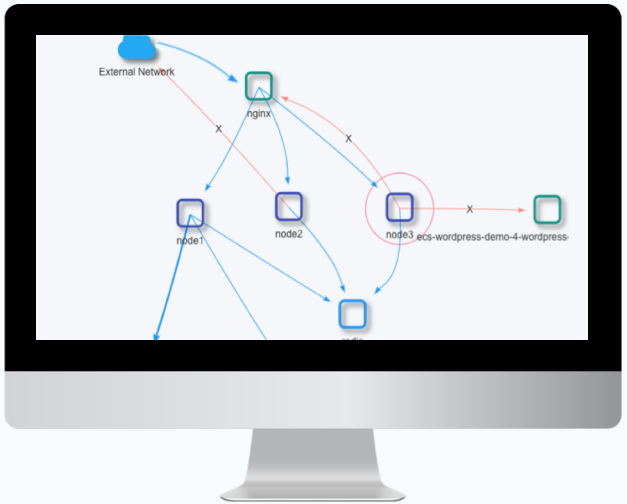
- L7 Network Security
- Endpoint Security
- Application Security

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