GlobalLogic®

GL DevOps Basecamp

Why do we need System Hardening?

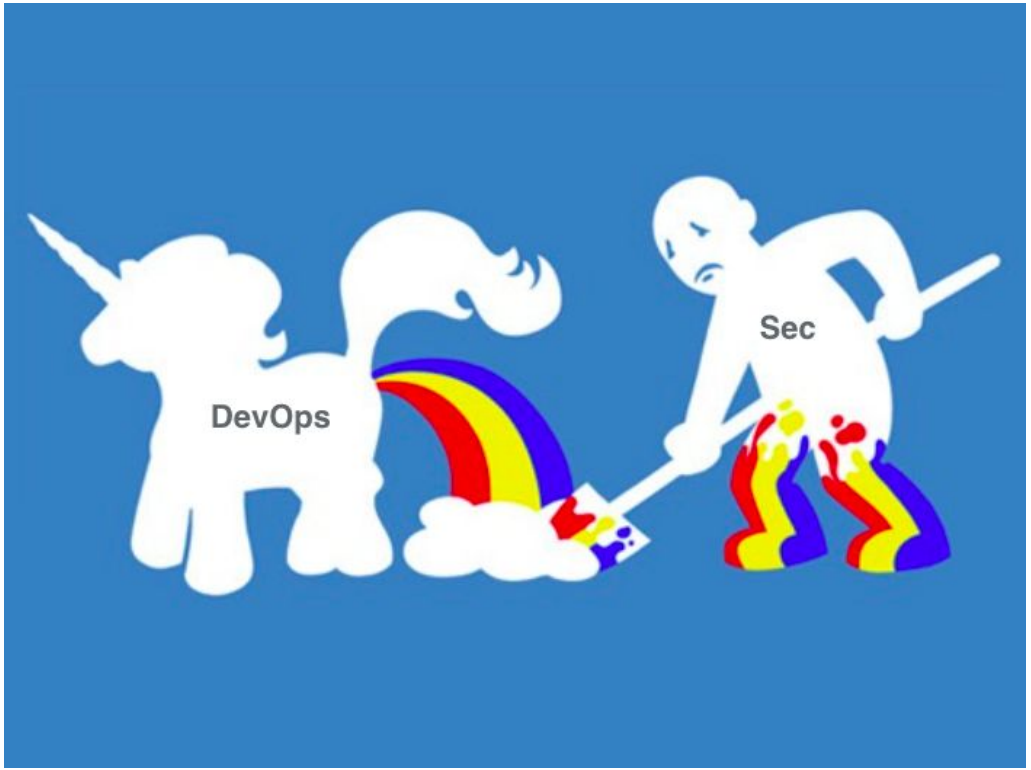
Alexander Adamov

PhD, Teaching at NURE, Ukraine and BTH, Sweden

The Head of Security Practice at GlobalLogic Ukraine

November 6, 2020

DevOps + Security = DevSecOps



Agenda

1. Overview of cloud threats
    - Cloud tenant threats
    - Cloud provider threats
    - Targeted attacks and APTs (Cloud Atlas, Cloud Hopper)
2. Defensive techniques
3. Cloud security architecture: DMZ, Security Domain
4. Kubernetes hardening
5. Monitoring, auditing, and incidents detection
6. Homework

Cloud threats overview

Cloud tenant threats

Insider threats (from a cloud provider):

- Cloud services misconfiguration
- A failure in maintenance.
  - For example, not wiping disks on nodes between re-allocations
- Improper configuration of security services or turning them off when high loaded.
  - For example, disabling rules and taking protocols out of scan by IDPS may lead to missing the attack.
- Connecting VMs to the management network.

Co-tenant threats

- Another tenant might try to escape a VM and take over the host.
- Getting access to shared resources such as storage, network, and so on.
- Another tenant might be taken over to run a DoS attack.
- Brute-force and dictionary attack.
- Shared cloud provider’s infrastructure such as:
  - a shared mail service may lead to spear-phishing attacks from one tenant to another
  - a shared DNS service may led to DNS poisoning attack
  - a shared Web service such as cloud admin web interfaces may be a source of XSS, CSRF, SQL injection, and so on attacks.

Cloud provider threats

A tenant to hack the provider:

- a tenant may run out of a VM or container using security breaches and get access to management network
- a fraud tenant can sign up using stolen credentials, for example, to organize a botnet, bitcoin miner, or Command-and-Control server that will be paid by the victim
- brute-force and dictionary attacks
- resource exhaustion

Malicious tenant behaviour that leads to blacklisting or loss of reputation of a cloud provider may include:

- Outgoing DDoS attacks
- Spamming
- Mining Bitcoins
- Distributing malware, pirated, or other illegal content

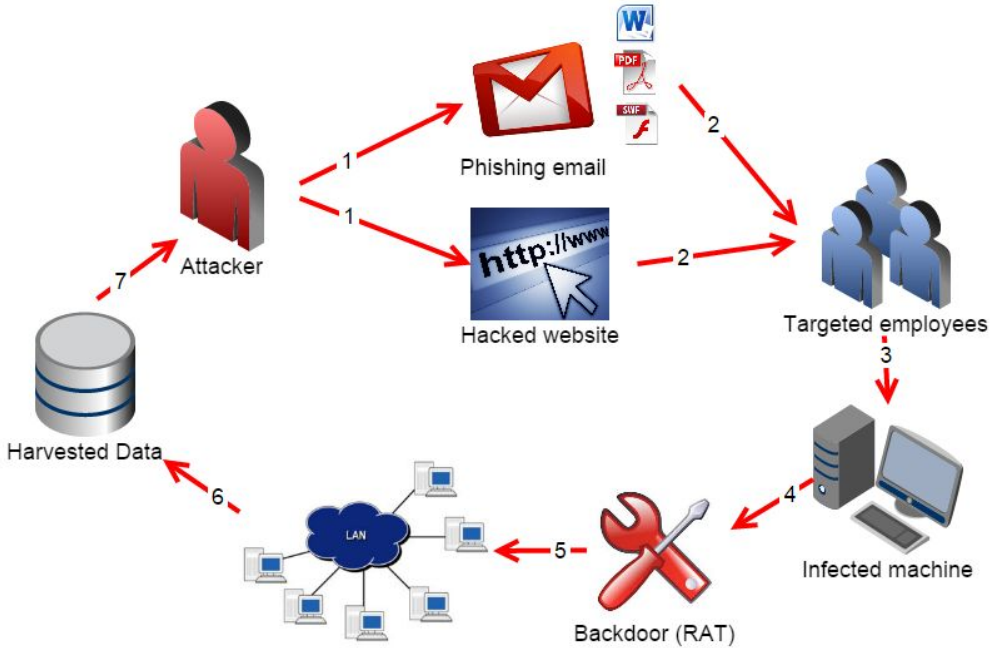
Outsider threats:

- Targeted Attacks
- DDoS
- Human-related threats:
  - insider access
  - social engineering
- Third parties access
- MITM and DoS attacks using BGP exposed to Internet access
- Vulnerabilities in network devices

Targeted attacks and APTs

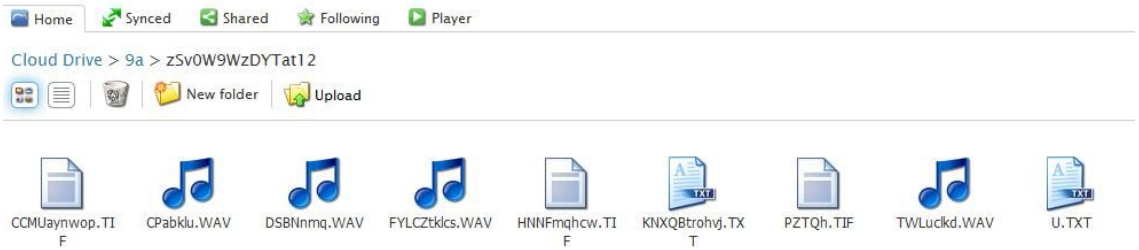
Targeted attacks can be executed via:

a. spear-phishing emails
b. watering hole attacks
c. 0-day exploits
d. brute force of RDP/SSH



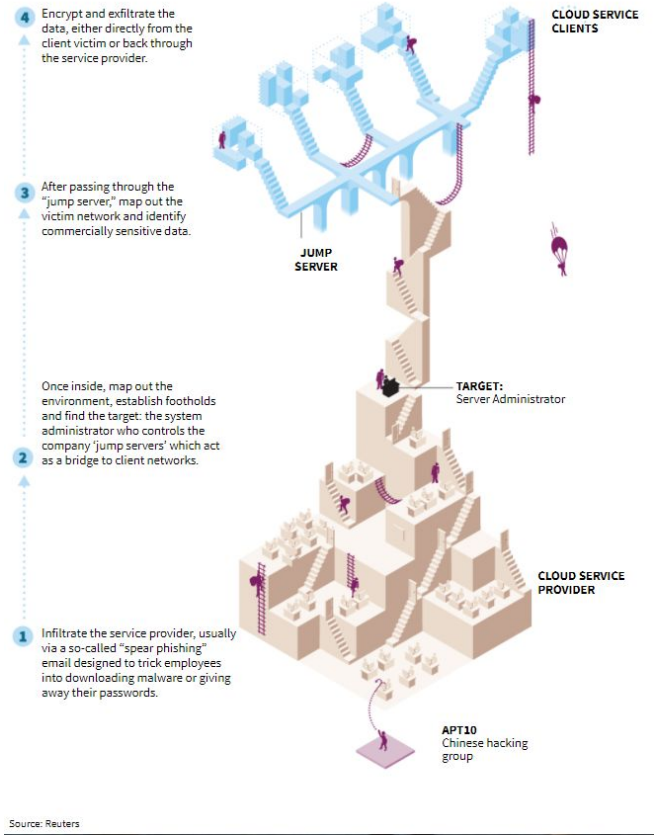
APT Cloud Atlas

- Attacker: ?
- Target: Russia
- Malware: Trojan.Win32.CloudAtlas, Trojan.Linux.Cloudatlas.a, Trojan.AndroidOS.Cloudatlas.a, Trojan.IphoneOS.Cloudatlas.a
- Delivery: spear-phishing with Microsoft exploit attached that dropped VB script
- C&C: at CloudMe ->



APT CloudHopper - 2017

- Attacker: APT10 from China
- Target: Managed IT Service Providers (MSPs)
- Malware: PlugX, Poison Ivy, ChChes, RedLeaves, Quasar
- Delivery: spear-phishing with '.exe' file attached

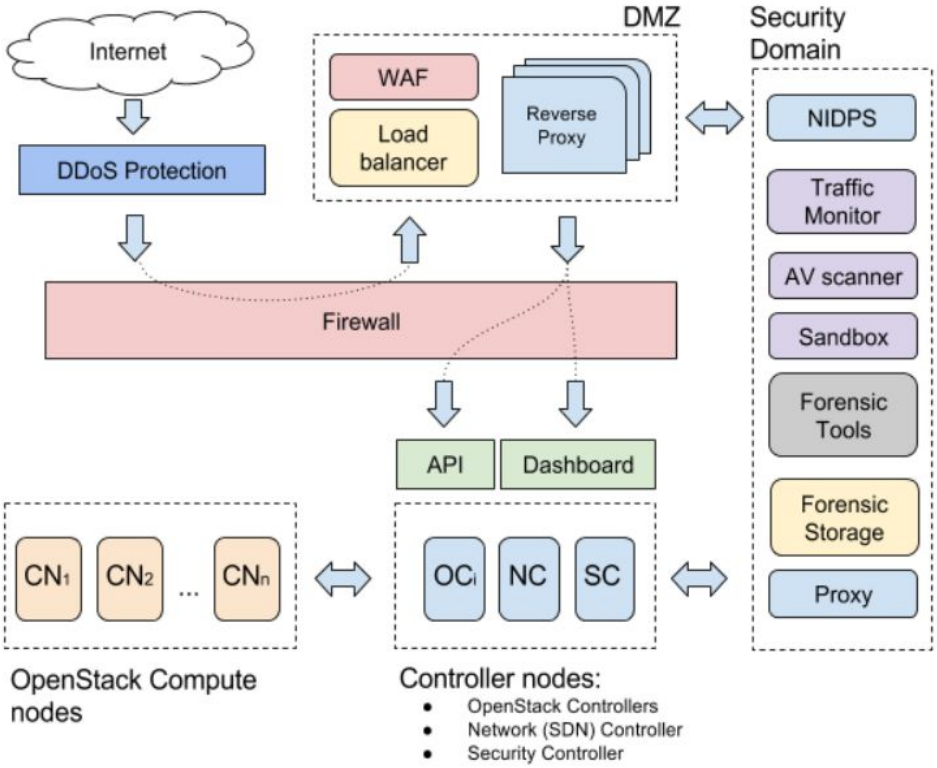


Defensive techniques

Defensive techniques

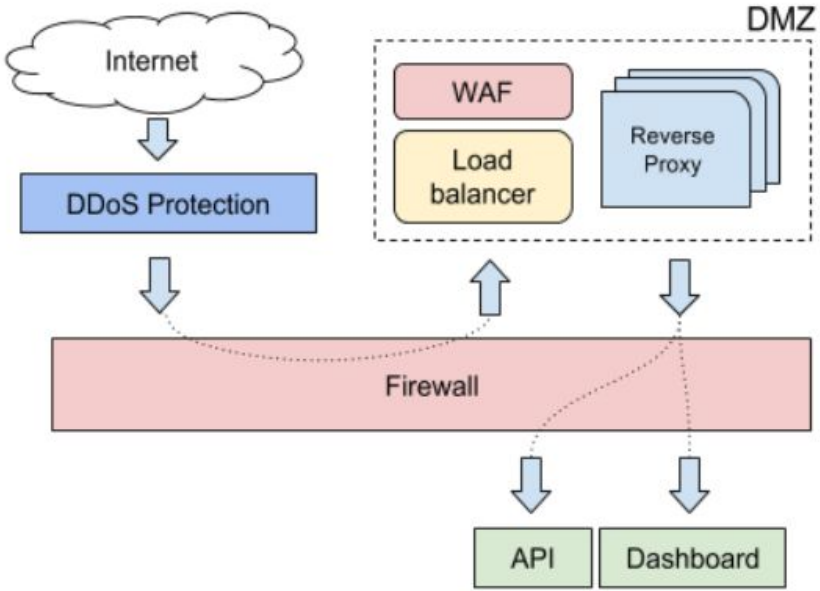
- TLS encryption
- Using digital certificates
- MAC, RBAC, ACL
- Logging, monitoring, and auditing
- Secret Manager
- Volume encryption
- Filtering, Quotas, Geo distribution
- Host Aggregates and Availability Zones

Secure Cloud Architecture



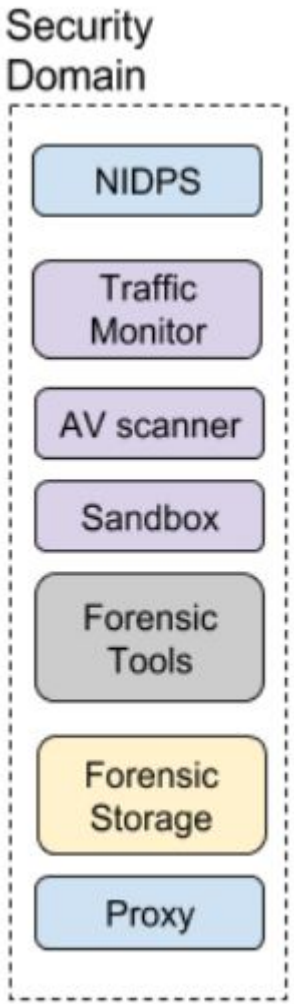
DMZ

Demilitarized zone (DMZ) - a neutral zone and aims to isolate private network from the Internet by including redundancy in cloud infrastructure. Recommended by NIST 800-44



Security Domain

Security Domain is a separate project with a set of tools needed for IRT to perform incident analysis and cloud forensics.



Hardening of Kubernetes

- Leverage Kubernetes ‘secrets’ and ‘federated secrets’ objects to hold sensitive information, such as passwords, OAuth tokens, and ssh keys.
- Verify that container images contain no vulnerabilities to mitigate the EoP threat.
- Limit access to Kubernetes nodes to mitigate the tampering and EoP threats.
- Limit scope of user permissions to mitigate the information disclosure, tampering, EoP, and DoS threats.
- Define resource quota to prevent the DoS attacks.
- Implement network segmentation to mitigate the EoP, DoS, tampering and information disclosure threats.
- Apply security context to mitigate the EoP, tampering, and information disclosure threats.
- Enable logging to mitigate the repudiation threat.

SIEM + SOC

SIEM (Security Information and Event Management)

- Chronicle
- LogRhythm
- Q-Radar from IBM
- Splunk
- OSSIM from AlienVault
- ArcSight from HP

SOC - Security Operation Center

Homework: Linux passwords hardening

Do not use your username in password

- Task:
    1. Create and run a script (Ansible playbook) to harden users' passwords by rejecting the ones that contain a username. Enforce this rule for 'root' as well.
    2. [Optional] Try to implement the same hardening rule without PAM.
    3. Write a report in Google Doc providing the playbook's code and proof of workability (screenshots or *asciicinema* recording)
- Target platform: any Linux-based distribution
- Tools
    1. Ansible (learn here)
    2. Utilize PAM authentication module

See also

- Free RedHat Ansible Training: https://www.redhat.com/en/services/training/do007-ansible-essentials-simplicity-automation-technical-overview?section=Overview
- CIS Benchmarks https://www.cisecurity.org/cis-benchmarks/
- DISA STIGs https://public.cyber.mil/stigs/
- SUSE https://documentation.suse.com/sles/11-SP4/single-html/SLES-hardening/index.html
- RHEL https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/chap-hardening_your_system_with_tools_and_services