Nation-state-Akteure und die Cloud?

Florian Hartmann, Cloud Subject Matter Expert

Agenda

- Intro
- Cloud Angrifssvektoren
- Highlights von staatlichen Akteuren
- Q&A

CROWDSTRIKE

Florian Hartmann
Cloud SME & Senior Sales Engineer

- Mehr als 20 Jahre IT / IT-Security Erfahrung
- Erfahrung im Bereich Netzwerk- und Endgeräteschutz
- 2 ½ Jahre bei CrowdStrike in Kundenprojekten zu allen Themen der CrowdStrike Plattform
- Mehrere Jahre Cloud Erfahrung und AWS Solutions Architect, CCSK

CLOUD HAS GONE MAINSTREAM

Gartner

"By 2025, more than 85% of global organizations will be running containerized applications in production, which is a significant increase from fewer than 35% in 2019."

Use of Kubernetes in production grew from 58% to 78% just between 2018 and 2019

Cumulative Docker Hub pulls nearly doubled in just the last six months

SECURITY ISSUES WITH CLOUD INFRASTRUCTURE

SHADOW IT

- Lack of Visibility
- Unauthorized Usage
- Unsecured Assets

CLOUD COMPLEXITY

- Misconfig/ Open Ports
- Many Tools / CI/CD
- Use of Insecure APIs

RUNTIME THREATS

- Adversaries
- APTs / Zero Day
- Vulnerabilities

SKILLS SHORTAGE

- IAM, Key Management
- Cloud / Security
- Shared Responsibility

CLOUD SERVICE PROVIDERS HAVE THE SAME PREDICAMENT

Researchers Call for 'CVE' Approach for Cloud Vulnerabilities

New research suggests isolation among cloud customer accounts may not be a given — and the researchers behind the findings issue a call to action for cloud security.

Kevin Beaumont ✓
@GossiTheDog

There is a massive gap in cloud security, by the way. No CVE numbers are issued for flaws, and suppliers aren't required to disclose flaws. Cloud services aren't magically secure.

You'll notice public disclosure of this comes from an external researcher.

Disrupted

EXCLUSIVE Microsoft warns thousands of cloud customers of exposed databases

By Joseph Menn

A federally contracted research lab tracks all known security flaws in software and rates them by severity. But there is no equivalent system for holes in cloud architecture, so many critical vulnerabilities remain undisclosed to users, Luttwak said.

INCREASING THREATS TO CLOUD ENVIRONMENTS

1. CLOUD VULNERABILITY EXPLOITATION
2. CREDENTIAL THEFT
3. CLOUD SERVICES PROVIDER ABUSE
4. USE OF CLOUD FOR HOSTING MALWARE & C2
5. EXPLOITATION OF MISCONFIGURED CONTAINERS

FANCY BEAR

COZY BEAR

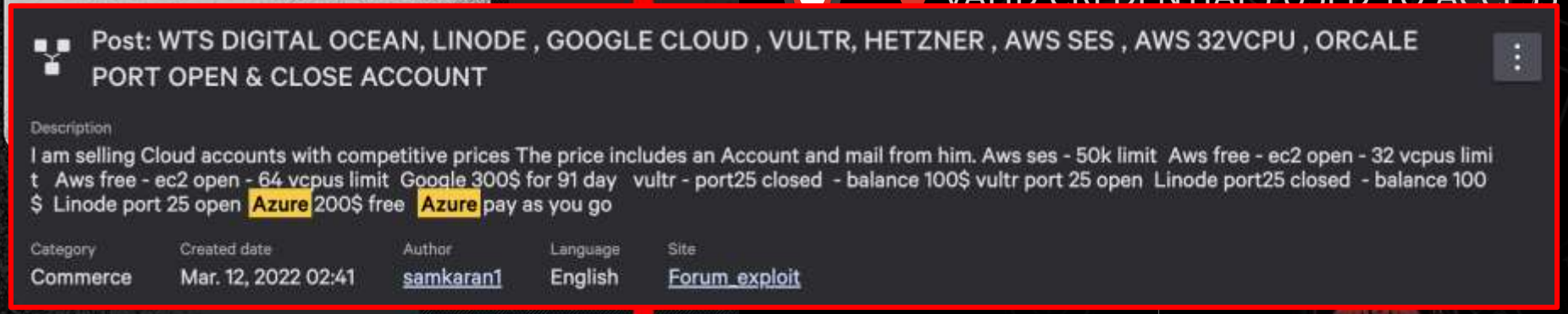
CROWDSTRIKE

CLOUD VULNERABILITY EXPLOITATION

- CVE IN CLOUD-BASED FILE TRANSFER APPLIANCES
- VMWARE CLOUD FOUNDATION

CREDENTIAL THEFT

- FAKE CREDENTIAL AUTHENTICATION PAGES TARGETING WEB MAIL PROVIDERS, OKTA, AND O365
- VALID CREDENTIALS USED TO ACCESS



Post: WTS DIGITAL OCEAN, LINODE , GOOGLE CLOUD , VULTR, HETZNER , AWS SES , AWS 32VCPU , ORCALE PORT OPEN & CLOSE ACCOUNT

Description

I am selling Cloud accounts with competitive prices The price includes an Account and mail from him. Aws ses - 50k limit Aws free - ec2 open - 32 vcpus limi t Aws free - ec2 open - 64 vcpus limit Google 300$ for 91 day vultr - port25 closed - balance 100$ vultr port 25 open Linode port25 closed - balance 100 $ Linode port 25 open Azure 200$ free Azure pay as you go

Category	Created date	Author	Language	Site
Commerce	Mar. 12, 2022 02:41	samkaran1	English	Forum_exploit

APRIL 2021

COSMIC WOLF TARGETS AWS ENVIRONMENT

ONGOING

ACCESS BROKERS

COMPROMISING TRUSTED THIRD PARTIES

- COMPROMISE CSP GLOBAL ADMIN ACCESS TO SECURE ACCESS TO NUMEROUS TENANTS
- COMPROMISE SUPPORT ACCOUNTS TO ENABLE VERTICAL PROPOGATION

ONGOING

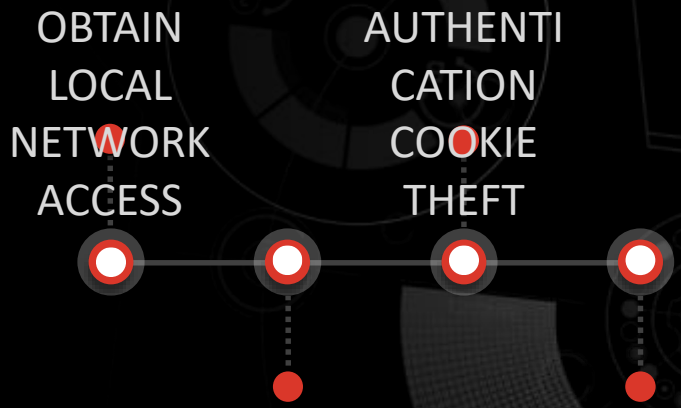
COZY BEAR

COMPROMISE O365 PROVIDERS TO ACCESS CUSTOMER TENANTS

- EMAIL AND FILES COMPROMISED AND EXFILTRATED

BYPASING MFA TO ACCESS CLOUD ENVIRONMENTS

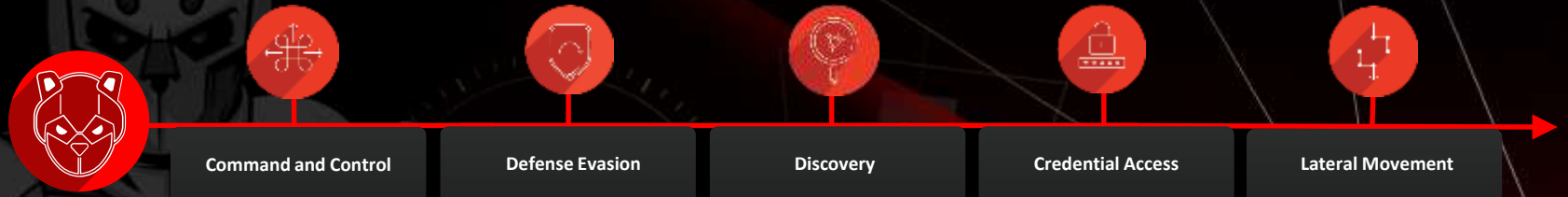
STELLARPARTICLE CAMPAIGN CONTINUES TARGETING **MSFT365**



Looking Deeper: Falcon OverWatch Case Study

PANDA Explores Linux and AWS Workloads Following Exploit of CVE

In April of 2022, OverWatch uncovered multiple interactive intrusions exploiting the CVE-2022-29464 vulnerability which allowed unrestricted file upload and remote code execution. These campaigns were consistent with China-nexus targeted intrusion activity. This case study details the TTPs observed in an intrusion against multiple Linux hosts at a technology entity.



Command and Control

The adversary used wget and curl to retrieve a selection of tooling from a remote IP which included fscan, cryptojacking tools, and multiple webshells including Godzilla and other .jsp variants commonly available on Chinese-language GitHub repositories.

Defense Evasion

The adversary deployed numerous anti-forensic efforts including the timestomping of webshell files with the aim of frustrating response and remediation efforts

Discovery

The adversary performed interactive reconnaissance which included the scanning of local subnets and identification of potential lateral movement targets. Additionally, the adversary installed the AWS command line utility awscli to facilitate advanced AWS reconnaissance and began enumerating AWS credential stores and configurations.

Credential Access

Continuing the hunt for credentials, the adversary inspected numerous sensitive files in search of credentials including /etc/shadow and .bash_history

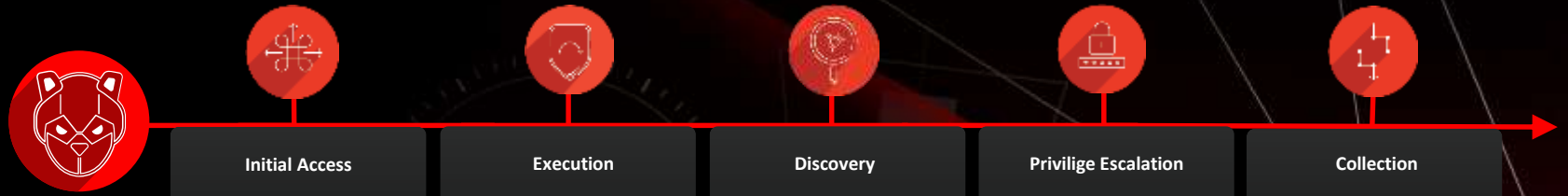
Lateral Movement

Finally, the adversary attempted lateral movement to multiple internal hosts via SSH.

Looking Deeper: Falcon OverWatch Case Study (2)

Unknown actor moves laterally within AWS VPC

In June 2022, CrowdStrike Falcon OverWatch observed hands-on-keyboard (HOK) activity by an unknown actor leading to the compromise of a host within an AWS Virtual Private Cloud (VPC) at a South Asian e-commerce company. The actor moved laterally within the VPC to an EC2 instance, dropped a RemCom sample, executed AWS reconnaissance commands, and stole temporary security credentials.



Initial Access

Initially, the actor accessed the AWS VPC host (H1) via unidentified means.

Execution

The actor leveraged this access to drop a common RemCom sample onto another host (H2) inside the VPC. When the execution of the RemCom sample was blocked, the actor used H1 to execute remote commands using WMI on H2.

Discovery

For reconnaissance, the actor listed the local users on H2 with net users and visible EC2 instances using aws ec2 describe-instances to discover additional hosts.

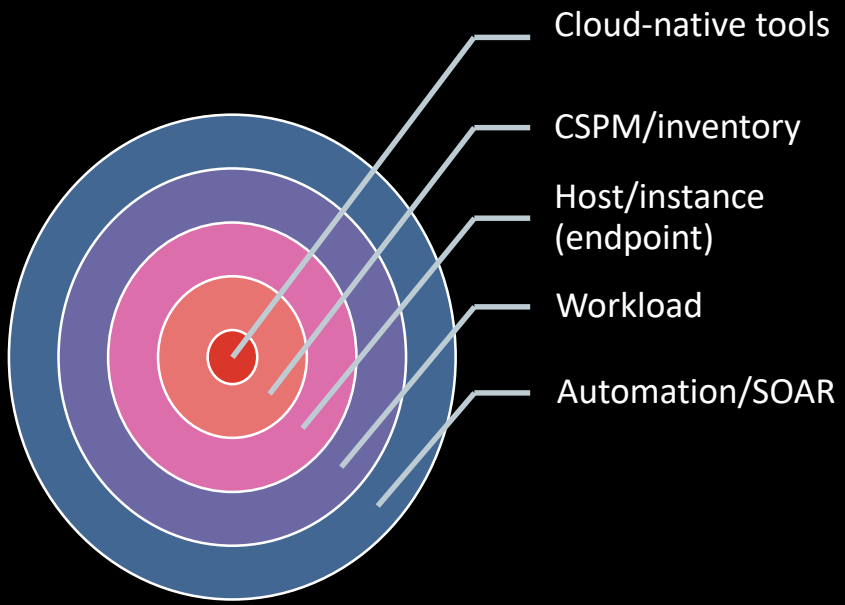
Privilige Escalation

Additionally, the actor executed the aws sts get-caller-identity command to retrieve the Identity Access Management (IAM) role—in particular the role name—attached to H2.

Collection

Knowing the role name, the actor reached out to the AWS instance metadata service—reachable via the link-local address 169.254.169[.]254—to retrieve the temporary security credentials of that role using curl http[:]//169.254.169[.]254/latest/meta-data/iam/security-credentials/<role_name>, in which <role_name> is the previously retrieved role name.

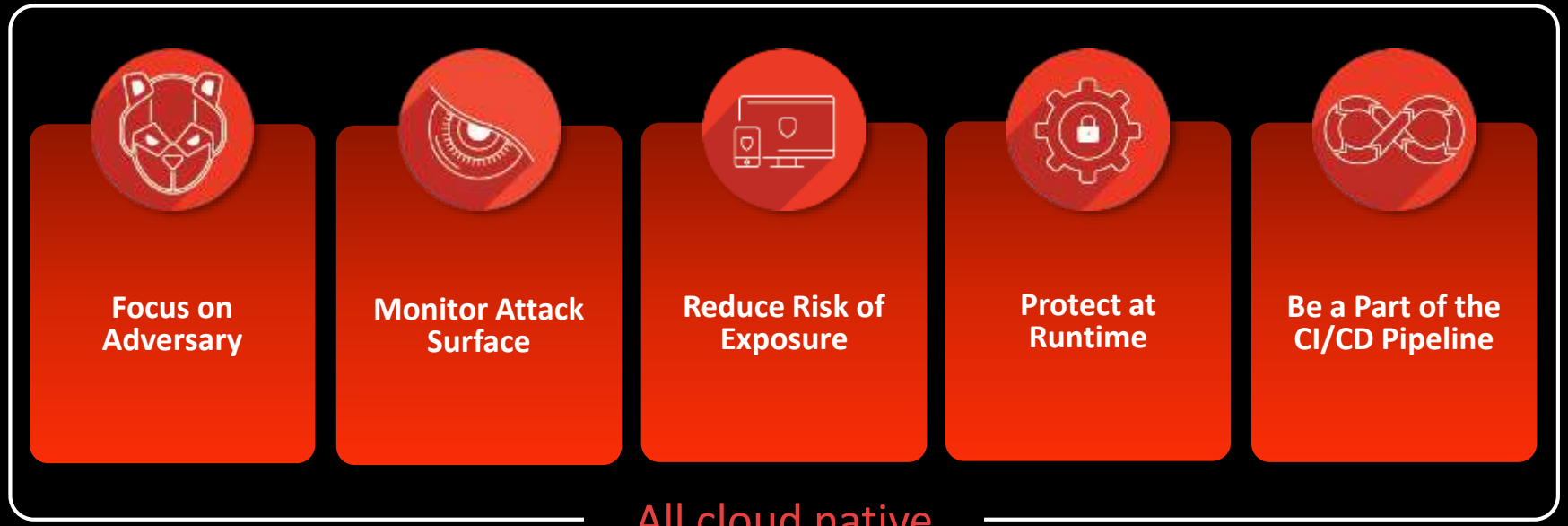
Defense in depth in the cloud? – Best Practise!



- Use the tools on best practice that are provided by CSP
- Enable runtime protection and obtain real-time visibility.
- Eliminate configuration errors.
- Leverage a CSPM solution.
  - Not just for Compliance, use it to harden the environment AND detect changes live and alert based on event streams and other technics.

CROWDSTRIKE

CrowdStrike approach to cloud security



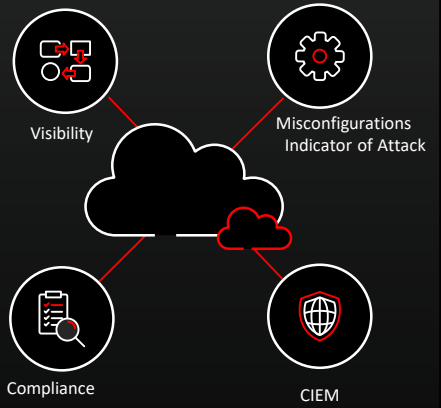
https://www.crowdstrike.com/blog/why-you-need-an-adversary-focused-approach-to-stop-cloud-breaches/

CROWDSTRIKE

Crowdstrike Cloud Security

Agentless Scanning…Agent-based Protection…One Platform

Agentless Cloud Security



Agent Runtime Protection

VM | Containers | Serverless

ML | IOA | NGAV | EDR | Vuln. Mgt. | Managed Hunting

Cloud Native Protection

Shift-Left - Image Assessment | RBAC | APIs
Workflows | Automatic Remediations

CNAPP for Continuous Compliance & Security

CROWDSTRIKE

Closing
&
Q&A