



Облачный пентест: Методики тестирования AWS

@allDisc0very



01

AWS Cloud 101

Преимущества и недостатки использования облачной инфраструктуры

Основные сервисы AWS, способы аутентификации, концепция Shared Responsibility Model

Легальный статус пентеста в облачной инфраструктуре AWS

02

Методики тестирования AWS

Эксплуатация типичных ошибок администрирования облачных сервисов AWS:

- Open S3 Buckets, Buckets Objects, S3 Code Injection & Hijacking
- Domain Hijacking
- EBS Volumes
- Docker & Kubernetes
- Уязвимые Web приложения
- Утечки ключей и учетных данных из Git-репозитория

03

Демо

Расу - AWS exploitation framework

04

Выводы и рекомендации

- Twitter: @allDisc0very
- Pentester @Digital Security
- Cloud Security Researcher
- Red Teamer Wannabe

Вадим Шелест

Аудитор информационной
безопасности

v.shelest@dsec.ru



Преимущества использования облачной инфраструктуры



Преимущества

- ✓ Стоимость – Оптимизация затрат на техническое обслуживание и персонал
- ✓ Безопасность – Комплексный подход к обеспечению безопасности на базовом физическом и сетевом уровне, соответствие стандартам и требованиям PCI, GDPR, and HIPAA
- ✓ Масштабируемость – Возможность увеличения и уменьшения количества используемых ресурсов в зависимости от текущих потребностей
- ✓ Гибкость - Возможность изменить технические характеристики и конфигурацию программного и аппаратного обеспечения оборудования.
- ✓ Надежность – Доступность ресурсов 99,99 % времени благодаря широкому географическому покрытию зон доступности, которые являются полностью изолированными частями инфраструктуры

Недостатки использования облачной инфраструктуры



Недостатки

✓ Монополия – Полная зависимость от конкретного провайдера облачных услуг относительно ценообразования и конкретных условий предоставления некоторых сервисов (kubernetes - master plane)

✓ “Легкость администрирования” – Простота развертывания и администрирования ресурсов в облачной инфраструктуре, благодаря нескольким щелчкам мышки в окне браузера, складывается обманчивое впечатление, что читать RTFM теперь совсем не обязательно

Доля рынка , основные продукты и сервисы AWS Amazon



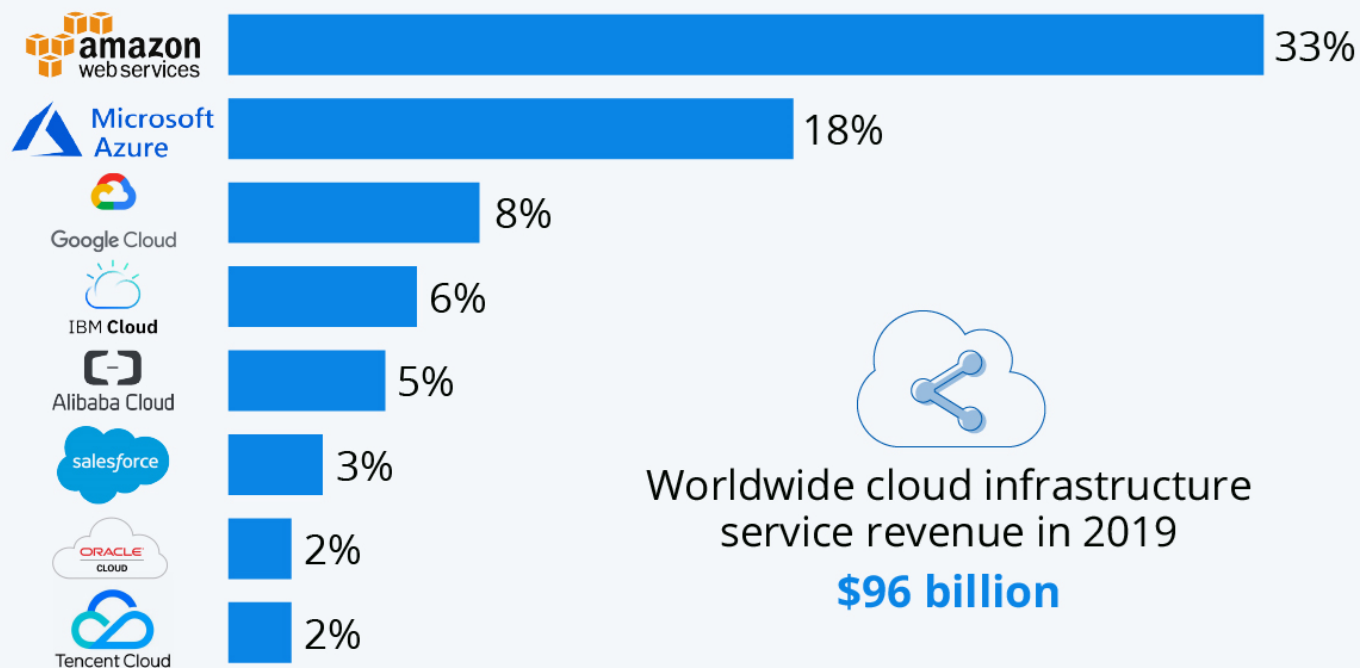
Amazon Web Services (AWS) – самая распространенная в мире облачная платформа.

Предоставляет более 175 полнофункциональных сервисов, таких как инструменты для облачных вычислений, хранилища и базы данных, инновационные возможности машинного обучения и искусственного интеллекта, озера данных и аналитики, а также Интернета вещей

Источник: [Synergy Research Group](#)

Amazon Leads \$100 Billion Cloud Market

Worldwide market share of leading cloud infrastructure service providers in Q4 2019*



Shared Responsibility Model

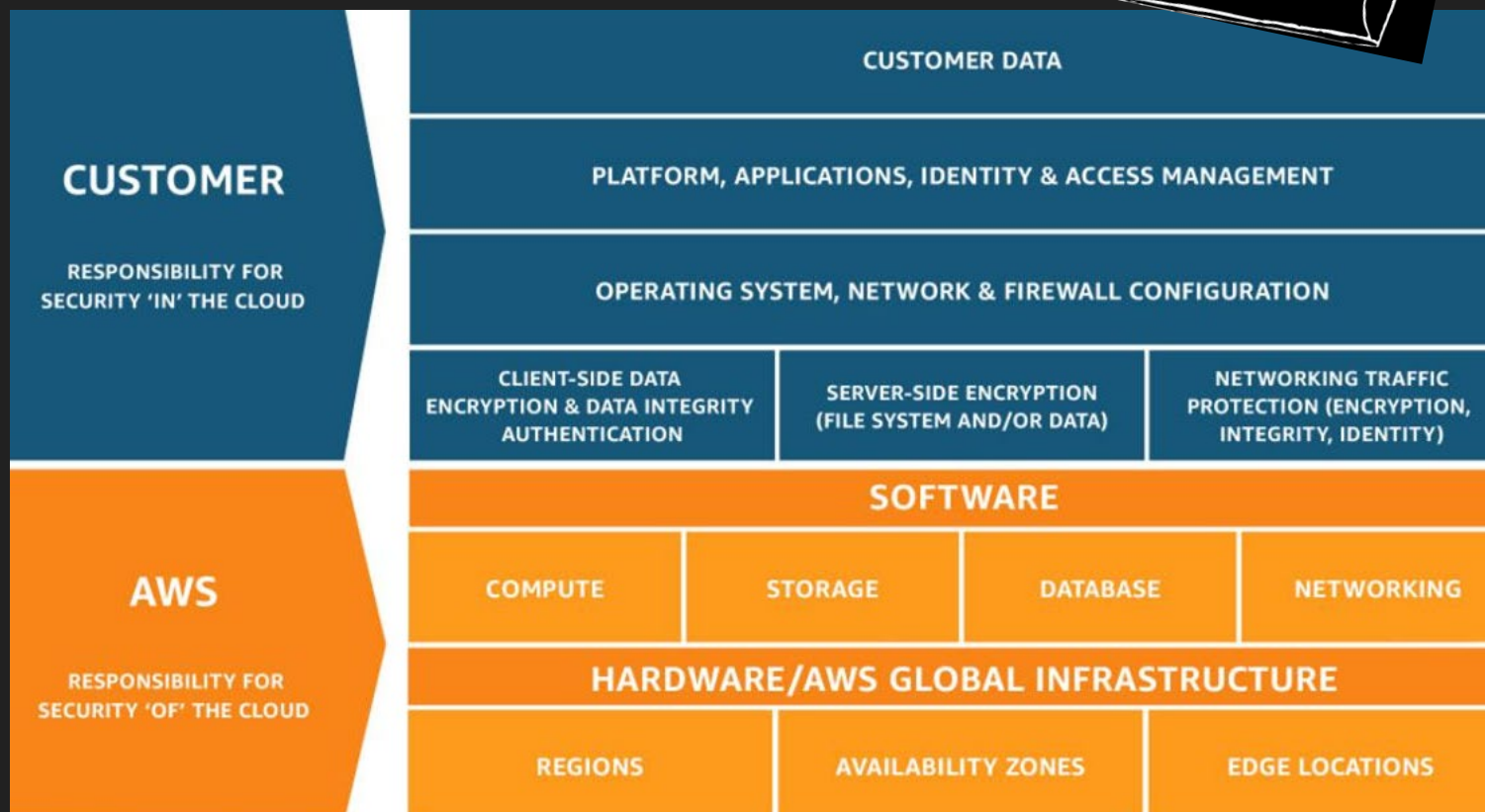
Модель распределенной ответственности AWS предполагает наличие двух параллельных зон ответственности:



AWS гарантирует безопасность Hardware и Software оборудования и комплектующих всех дата-центров глобальной инфраструктуры AWS



Клиент несет ответственность за обеспечение безопасного использования операционных систем, систем сетевого контроля и взаимодействия платформ и приложений, систем управления доступом и других пользовательских данных в процессе хранения и транзита в облаке



AWS Pentest Authorization



С 2019 года в AWS упростили процедуру получение разрешения на тестирование, больше не нужно заполнять многочисленные регистрационные формы, согласовывать время и предоставлять IP-адреса атакующих <https://aws.amazon.com/security/penetration-testing/>

AWS Customer Support Policy for Penetration Testing

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services, listed in the next section under "Permitted Services."

Customer Service Policy for Penetration Testing

Permitted Services

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Prohibited Activities

- DNS zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

Эксплуатация типичных ошибок администрирования сервисов AWS



MITRE ATT&CK AWS Matrix

MITRE | ATT&CK®

[Matrices](#) [Tactics ▾](#) [Techniques ▾](#) [Mitigations ▾](#) [Groups](#) [Software](#) [Resources](#)

Search 🔍

AWS Matrix

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the AWS platform.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Collection	Exfiltration	Impact
Exploit Public-Facing Application	Account Manipulation	Valid Accounts	Redundant Access	Account Manipulation	Cloud Service Dashboard	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Trusted Relationship	Create Account		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Data from Information Repositories		
Valid Accounts	Implant Container Image		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning	Data from Local System		
	Redundant Access		Valid Accounts		Network Share Discovery	Data Staged		
	Valid Accounts				Remote System Discovery			
					System Information Discovery			
					System Network Connections Discovery			

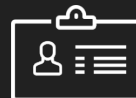
Способы аутентификации



Programmatic

Используется для аутентификации через AWS API, CLI, SDK и других средств разработки

AWS Access Key ID: ASIAXCQKGTUXQPDESVDQ
Secret Access Key: wfZDhTYlFeaJK*****



Management Console

Используется для аутентификации на веб-портале <https://signin.aws.amazon.com>

Имя пользователя: happy_amzn_user
Пароль: complex_amzn_pass2020!



Programmatic access

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.



AWS Management Console access

Enables a **password** that allows users to sign-in to the AWS Management Console.

Ошибки конфигурации AWS S3 Buckets

Open S3 Buckets



Amazon Simple Storage Service (S3) – сервис, позволяющий хранить и получать данные любого объёма, в любое время из любой точки сети.

Безопасен “по умолчанию”... пока администратор не включил публичный доступ...

S3 URL:

- [https://\[bucketname\].s3.amazonaws.com](https://[bucketname].s3.amazonaws.com)
- [https://s3-\[region\].amazonaws.com/\[Org Name\]](https://s3-[region].amazonaws.com/[Org Name])

S3 AWS CLI:

- [aws s3 ls s3://<bucketname>/ --region <region>](#)

Узнать конкретный регион можно с помощью nslookup

Bucket settings for Block Public Access

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Включено по умолчанию!

☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through **new** access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ Block public access to buckets and objects granted through **any** access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ Block public access to buckets and objects granted through **new** public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ Block public and cross-account access to buckets and objects through **any** public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

- ☐ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Ошибки конфигурации AWS S3 Buckets Objects

S3 Buckets Objects



Объекты, которые хранятся в S3 бакетах, тоже могут быть открыты для публичного доступа, даже при условии, что сам бакет закрыт.

Для этого достаточно знать S3 URL и наименования вложенных объектов. Адреса S3 часто можно найти в исходном коде приложений, а имена файлов можно подобрать с помощью классического брут-форса по словарю.

S3 buckets

Search for buckets

+ Create bucket Edit public access settings Empty Delete

Bucket name	Access
<input type="checkbox"/> all-your-base	Public
<input type="checkbox"/> cf-templates-83s6e9he54cx-us-east-1	Objects can be public
<input type="checkbox"/> cf-templates-83s6e9he54cx-us-west-2	Objects can be public
<input type="checkbox"/> config-bucket-989506195794	Objects can be public
<input type="checkbox"/> customer-records	Error

WTF?

Overview Properties Permissions Select from

Access for object owner

Canonical ID	Read object	Read object permissions
<input type="radio"/> 3161d233 58410fdb1bfd4735a18 (Your AWS account)	Yes	Yes

Access for other AWS accounts

+ Add account Delete

Canonical ID	Read object	Read object permissions
--------------	-------------	-------------------------

Public access

Group	Read object	Read object permissions
<input type="radio"/> Everyone	Yes	-

Ошибки конфигурации AWS S3 Buckets - Code Injection

S3 Code Injection



Сервис S3 также часто используется для хостинга статических веб-приложений, HTML-страниц, объектов JavaScript, картинок, видео и пр.

В случае неправильной конфигурации прав на запись файлов в S3 возможна инъекция вредоносного JavaScript кода в уязвимое веб-приложение, который будет выполнен в браузерах посетителей:

- XSS атаки
- Beef Hooks
- JavaScript майнеры криптовалют
- JavaScript Key logger
- ...

Cryptocurrency Web Miner Script Injected into AOL Advertising Platform

Posted on: April 4, 2018 at 5:30 am Posted In: Bad Sites Author: Trend Micro



by Chaoying Liu and Joseph C. Chen

On March 25, we saw that the number of cryptocurrency web miners detected by the Trend Micro Smart Protection Network suddenly spiked. Our team tracked the web miner traffic and found that the bulk of it was linked to MSN[.]com in Japan. Further analysis revealed that malicious actors had modified the script on an AOL advertising platform displayed on the site to



New Magecart attacks leverage misconfigured S3 buckets to infect over 17K sites

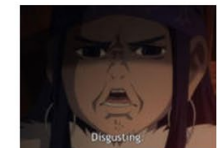
Web card skimming group takes a "pray-and-spray" shotgun approach to breaking into online stores.



By Catalin Cimpanu for Zero Day | July 11, 2019 -- 09:14 GMT (10:14 BST) | Topic: Security



MORE FROM CATALIN CIMPANU



Security
For 8 years, a hacker operated a massive IoT botnet just to download Anime videos



Tech Industry
Facebook fixes bug that crashed major iOS apps like TikTok, Spotify, and Tinder

Ошибки конфигурации AWS S3 Buckets - Domain Hijacking

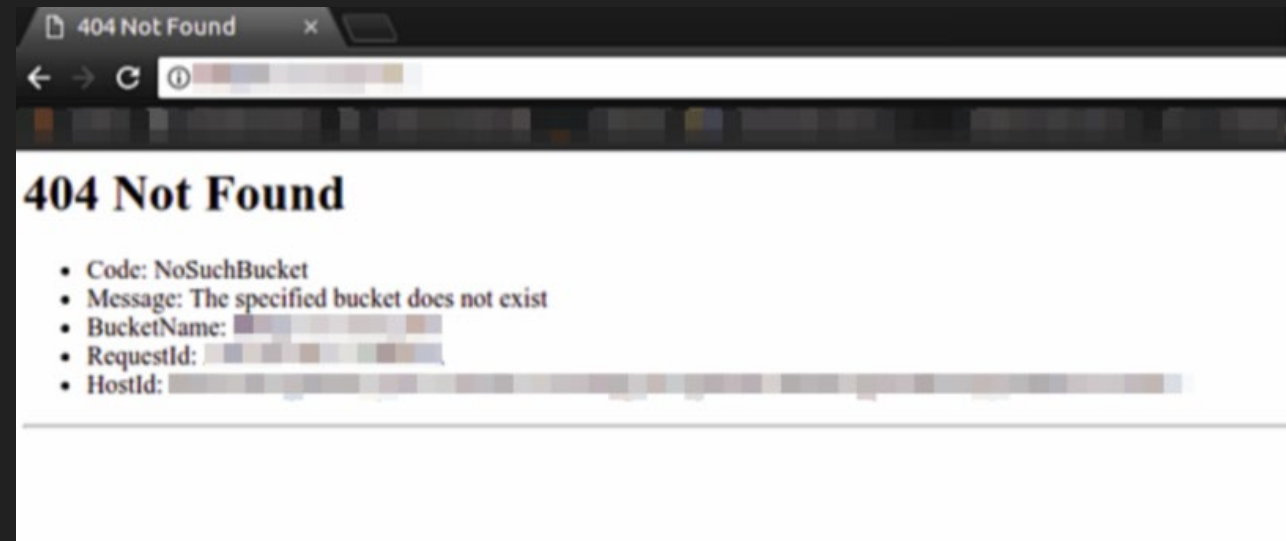
S3 Domain Hijacking



Вероятность захвата домена возникает, если приложение ссылается на S3 бакеты, которые были удалены и больше не существуют.

Так же довольно часто встречаются поддомены, которые имеют актуальную CNAME dns-запись, указывающую на S3 бакет, который был удален.

Для захвата таких доменов и поддоменов необходимо всего лишь создать новый S3 бакет с таким же именем и в том же регионе AWS. Поэтому крайне важно обращать внимание на 404 страницы на *.s3.amazonaws.com при брутфорсе поддоменов тестируемой организации



Поиск уязвимых AWS S3 Buckets

S3 Buckets Recon



Ручной поиск во время анализа веб-приложения.
В Burp Suite проверить приложение на запросы:

- [\[bucketname\].s3.amazonaws.com](#)
- [s3-\[region\].amazonaws.com/\[target-name\]](#)

Поиск объектов содержимого закрытых S3 бакетов, которые ранее были открыты и проиндексированы поисковиками, используя Google dorks:
[site:s3.amazonaws.com filetype:gzip backups](#)

Также для этой цели можно использовать индекс архивов сервиса [WayBackMachine](#)

Бесплатный онлайн-сервис по поиску S3 бакетов и их содержимого [GrayhatWarfare](#)

The screenshot shows the GrayhatWarfare website. At the top is the logo "GRAYHAT WARFARE" with the tagline "cause white is boring". Below the logo is a navigation bar with links: Home, Filter Buckets, Search Files, Docs / API, Top Keywords, Packages, FAQ, and Contact Us. A search bar is located on the right. The main content area displays statistics: "Files 1,631 of 3,976 million (?)", "Buckets 87136 of 259797 (?)", and "Last Update 28-April-2020". At the bottom, there is a "Search Public Buckets" section with a "Random Files" button.

Results for "backup"

#	Bucket	Filename
1	cuwebsite.s3.amazonaws.com ✖	wp-content/themes/ninezeroseven
2	resources-blue.s3.amazonaws.com ✖	assets/less/icons/material-design-
3	resources-blue.s3.amazonaws.com ✖	assets/less/icons/material-design-
4	wpcom.s3.amazonaws.com ✖	wp-content/uploads/2018/10/2316

Ошибки администрирования Elastic Block Store

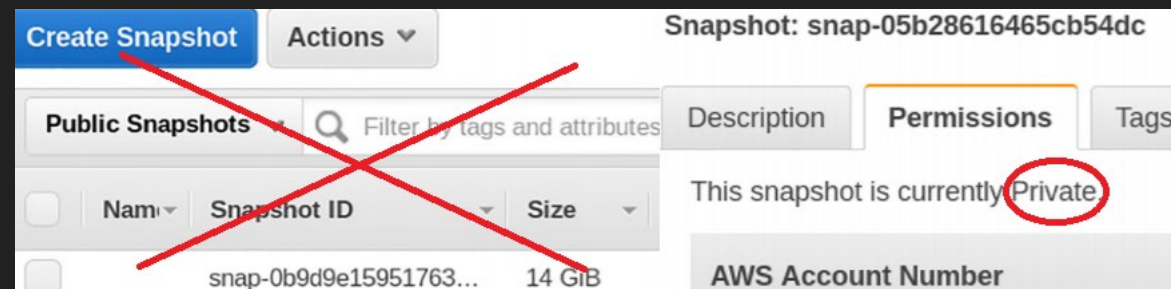
Elastic Block Store (EBS)



Amazon Elastic Block Store (EBS) – это сервис блочного хранилища, созданный для использования совместно с EC2. Обеспечивает пропускную способность и интенсивность транзакций рабочих нагрузок при любом масштабе.

Другими словами, это виртуальный жесткий диск для EC2, который тоже может быть доступен публично, в случае неправильной конфигурации, аналогично сервису S3.

Snapshot публичного EBS-volume может быть примониторван к любому EC-2 инстансу в том же регионе, далее обычным поиском по директориям можно найти много интересного. Например, AWS Root Keys, SSH Private Keys, Креды (SQL, API, Oath Tokens, VPN, etc/shadow) и пр.



			US East (Ohio)
<input type="checkbox"/>	shadow_8b0ed108a45267d1f5365da665d9dfd2_vol-04d	Jan 15, 2020 11:02:57 AM GMT-0700	995.0 B
<input type="checkbox"/>	shadow_8ba70862be90ce222cbe0e0708ae0e54_vol-03	Jan 15, 2020 10:59:32 AM GMT-0700	804.0 B
<input type="checkbox"/>	shadow_8cdb73aebad0e0f4a5d1933e83171ee6_vol-00	Jan 15, 2020 11:08:49 AM GMT-0700	896.0 B
<input type="checkbox"/>	shadow_8d4555024d621d92ab620a7715299be5_vol-03	Jan 15, 2020 11:05:55 AM GMT-0700	850.0 B
<input type="checkbox"/>	shadow_926828ca3bf10643fbcf95da8e06a884_vol-0d4	Jan 15, 2020 11:03:06 AM GMT-0700	850.0 B
<input type="checkbox"/>	shadow_932e0147af322f57d2459c7363969365_vol-0b4	Jan 15, 2020 10:57:04 AM GMT-0700	850.0 B
<input type="checkbox"/>	shadow_944d1b8579994529c0c2593088f6c2_vol-0b3	Jan 15, 2020 11:08:27 AM GMT-0700	850.0 B
<input type="checkbox"/>	shadow_947bf87649f97ab5f7139a997a45e5ff_vol-04c1	Jan 15, 2020 11:08:09 AM GMT-0700	850.0 B
<input type="checkbox"/>	shadow_94ac3b430e6654318bc793f87f474919_vol-0d9	Jan 15, 2020 11:07:21 AM GMT-0700	845.0 B

Для автоматизации можно использовать [Dufflebag](#). Легко разворачивается с помощью Elastic Beanstalk, автоматически монтирует образы публичных снапшотов, ищет возможные секреты и ключи, сохраняет найденное в S3

Ошибки администрирования Docker контейнеров на AWS

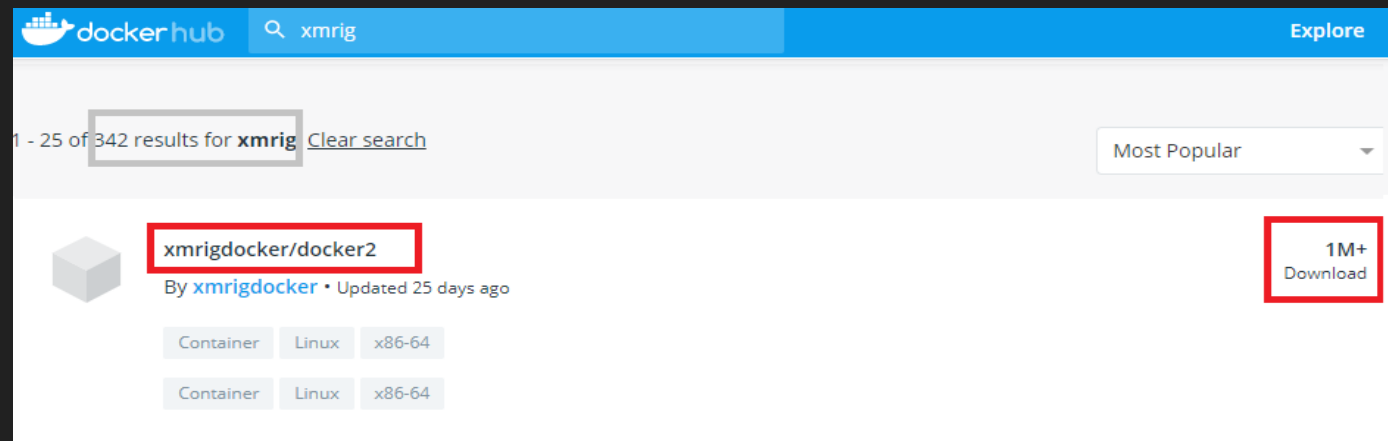
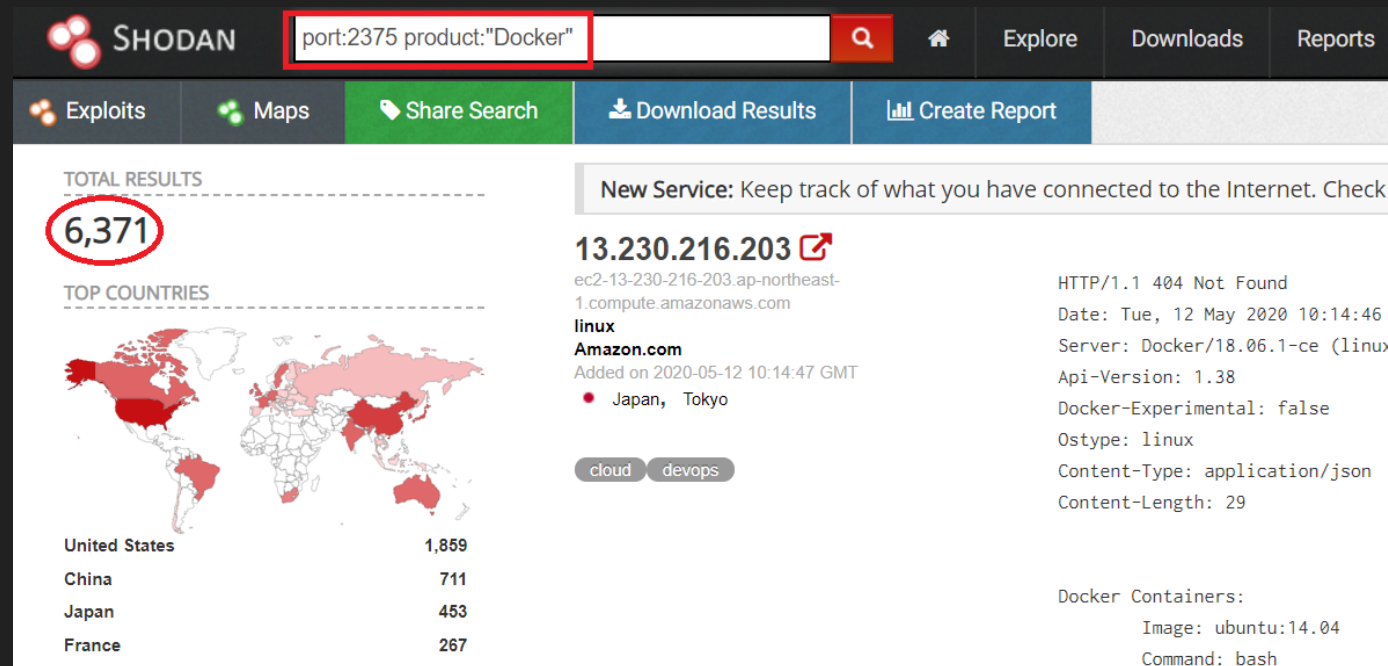
Containers (Docker)



Контейнеры – основа концепции современных DevOps. Используются для создания, интеграции и запуска приложений и сервисов в облачной инфраструктуре.

Неправильная конфигурация Docker Remote API на портах tcp/2375 и 2376 на публично доступном интерфейсе может привести к компрометации хоста.

Данные Shodan на май 2020: **739 хостов из 6371** уязвимы и активно используются для майнинга криптовалют. Более того злоумышленники активно используют сервис DockerHub, для размещения образов ПО для майнинга.



Ошибки администрирования кластеров Kubernetes на AWS

Containers (Kubernetes)



kubernetes

Доступный публично Kubernetes Management API на tcp/10250 и 10255 может привести к раскрытию информации о конфигурации кластера.

Доступный публично Kubernetes etcd API на tcp/2379 <http://<kubernets IP>:2379/v2/keys/?recursive=true>

Может привести к утечке AWS Keys, сертификатов, ключей шифрования и прочей чувствительной информации из хранилища etcd.

SHODAN search results for `port:10250 product:"Kubernetes"`. The search returned 1,157 results. The top result is for IP 137.74.42.172, identified as OVH SAS, located in France. It shows a devops self-signed SSL certificate issued on 2020-05-12. The interface includes tabs for Exploits, Maps, Share Search, Download Results, and Create Report.

Country	Count
China	476
United States	252

SHODAN search results for `port:2379 product:"etcd"`. The search returned 2,429 results. The top result is for IP 106.14.199.103, identified as Hangzhou Alibaba Advertising Co., Ltd., located in China. It shows an etcd service with Name: s1, Version: 3.3.8, and Uptime: 15859h4m9.442891911s. The second result is for IP 160.85.252.214, identified as Swiss Education and Research Network, located in Switzerland. It shows an etcd service with Name: mao0 and Version: 3.2.17. The interface includes tabs for Exploits, Maps, Share Search, Download Results, and Create Report.

Country	Count
China	1,081
United States	377
South Africa	234

Уязвимости Web приложений на AWS

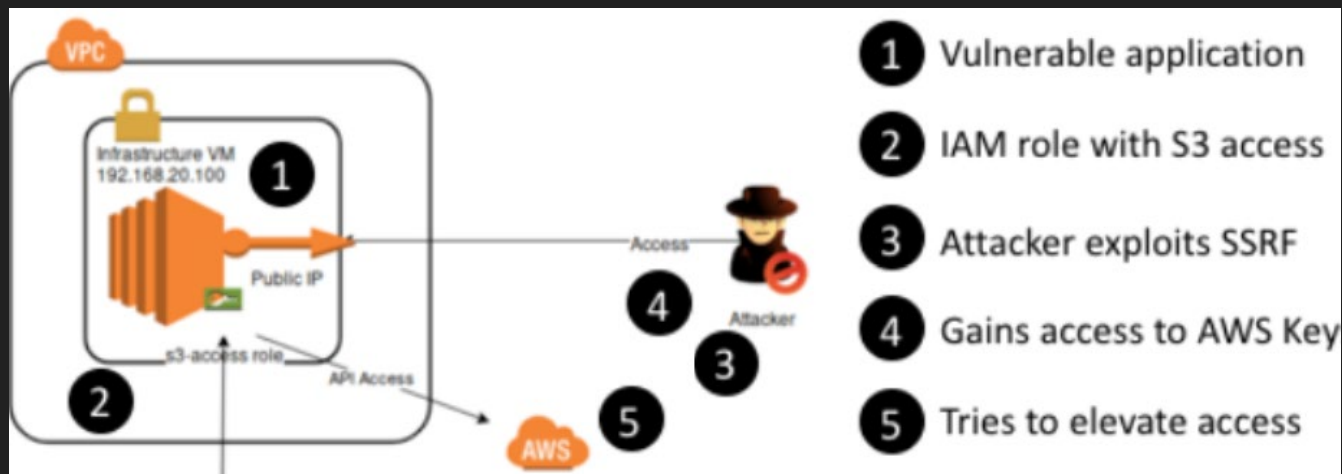
SSRF Vulnerability



В марте 2019 г. произошла утечка персональных и финансовых данных более 100 млн клиентов банка Capital One. Злоумышленник получил доступ к AWS S3 хранилищу, с помощью эксплуатации SSRF уязвимости на публичном сайте банка. Уязвимый веб-сервер позволял сделать запрос к сервису AWS Instance Meta Data Service (IMDSv1) по адресу:

<http://169.254.169.254/latest/meta-data/iam/security-credentials/>, чтобы получить AWS Keys приложения с правами доступа к S3 бакетам данных клиентов банка.

*В декабре 2019 г. AWS анонсировал IMDSv2, защищенный от подобных атак. Но по статистике на апрель 2020 г., лишь 4% клиентов используют IMDSv2.



Уязвимости Web приложений на AWS (продолжение)

Local File Inclusion (LFI)



Local File Inclusion (LFI) - это возможность чтения и выполнения локальных файлов на серверной стороне. Уязвимость позволяет получить доступ к файлам, содержащим переменные окружения учетных данных AWS на сервере

Linux:

[/root/.aws/credentials](#)
[/home/USERNAME/.aws/credentials](#)

Windows:

[C:/Users/USERNAME/aws/credentials](#)

Symfony PHP Framework, в режиме dev mode позволяет получить доступ к debug-компоненту - web profiler, раскрывающему чувствительную информацию (routes, cookies, credentials, files и пр.)

```
root:~# curl http://[redacted]/?file=/root/.aws/credentials
[default]
aws_access_key_id=AK[redacted]KA
aws_secret_access_key=e[redacted]
```

Variable	
USER	www-data
HOME	/var/www
APP_ENV	dev
APP_SECRET	[redacted]
AWS_KEY	[redacted]
AWS_SECRET	[redacted]
AWS_REGION	us-east-1
AWS_BUCKET_NAME	[redacted]
GEO_IP2_PATH	/var/[redacted]
REDIS_URL	redis://[redacted]
OPEAPIASDISPATCHER_NAME	banner-group-vpc-as
OPEAPIASDISPATCHER_SECRET	[redacted]
DATABASE_URL	postgres://[redacted]
SYMFONY_DOTENV_VARS	APP_ENV,APP_SECRET,AWS_KEY,AWS_IS_URL,OPEAPIASDISPATCHER_NAME,
SHELL_VERBOSITY	3

Эксплуатация типичных ошибок использования и хранения AWS Keys

Утечка ключей AWS из публичных репозиториев



```
@@ -57.8 +57.8 @@ public class EurekaEVCacheTest extends AbstractEVCacheTest
props.setProperty("datacenter", "cloud");
props.setProperty("awsAccessId", "<aws access id>");
props.setProperty("awsSecretKey", "<aws secret key>");
props.setProperty("awsAccessId", "AKIAJCK2WUHJ2653GNBQ");
props.setProperty("awsSecretKey", "7JyrN0rk23B7bErD88eg8IfhYjAYdFJlhC
props.setProperty(".appinfo.validateInstanceId", "false");
```

Разработчики очень часто “забывают” пароли, API-ключи, OAuth-токены и др. секреты, в том числе AWS Keys в публичных Git-репозиториях на Github, Gitlab и Bitbucket.

Автоматизированные инструменты для поиска:

- [Gitrob](#)
- [GitGot](#)
- [Gitleaks](#)
- [GitMiner](#)
- [TruffleHog](#)

* В 2019 году Github запустил сервис сканирования репозиториев на утечки ключей и др. секретов.



VS



GitGuardian

Эксплуатация типичных ошибок использования и хранения AWS Keys


Утечка ключей AWS из публичных репозиториев



[Shhgit live v0.3](#)

Сервис поиска утечек AWS Keys и других секретов
В режиме реального времени в веб-интерфесе:

*За период 48 часов автору инструмента удалось
найти
117 AWS Ключей , из них 58 оказались валидными, из
них 21 были ключам Root-аккаунтов на AWS



shhgit live! v0.3

294 matches 6 filters x

Potential private key (.asc) 117

Potential private key (.pem) 55

High entropy string 46

☒ Interesting file extensions ☒ High entropy strings ☐ Noti

Read the corresponding [blog.post](#) that inspired this tool.

Found	Signature Name	Matches
2:11:51 PM	AWS Access Key ID Value	AKIAT73L2G4503KS52Y5 AKIAT73L2G4503KS52Y5
1:39:54 PM	AWS Access Key ID Value	AKIAJOP4E4KWP3XYGMEA

Secret Type	Count	Verified
Username and Password in URI	1,351	440
Amazon AWS	117	58
Google OAuth keys	231	174
MailGun API keys	194	87
Slack Webhook URLs	139	62
SQLite databases	33	- *

[Pacu - AWS exploitation framework](#)

Модули:

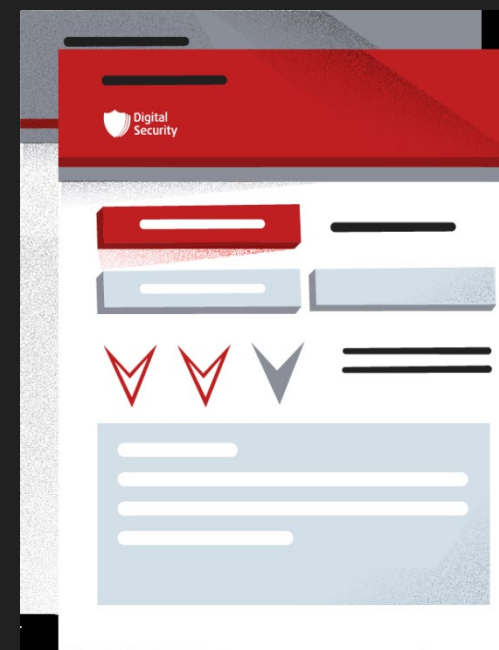
- EC2 enumeration
- IAM privilege escalation
- Persistence modules
- S3 bucket discovery



Рекомендации и выводы

AWS Security Best Practices:

- > НИКОГДА не использовать ключи Root аккаунтов
- > Multi-factor authentication (MFA) для Web Console и AWS Access keys
- > Надежные пароли или парольные фразы, там где невозможно MFA
- > Аудит и мониторинг IAM доступа, с помощью AWS IAM Access Analyzer или [Security Monkey](#)
- > IAM Roles (short-term temporary credentials) вместо IAM Users
- > Git-hooks для мониторинга и автоматического блокирования утечек секретов
- > Регулярная ротация AWS IAM Users Access keys, там где невозможно использовать IAM Roles
- > Zero trust и принцип наименее привилегированного доступа
- > Strong Application Security и регулярное проведение тестирований на проникновение



Questions?



Twitter: @allDisc0very

Email: v.shelest@dsec.ru