

How to run a real-world attack on cloud and protect from it

@Rootcon 2024

by Niko Akatyev

27th Sep 2024

[HORANGI](#). A BITDEFENDER COMPANY.



Speaker Intro.

Creating a safer cyberspace

Nikolay “Niko” Akatyev

As the Vice President of Security, IT, Compliance, Niko drives the internal machine that powers Horangi's efforts in contributing to a safer cyberspace. He is a regular speaker and contributor in the international cybersecurity community, from Asia to the Caribbean.

Work experience

- Horangi, a Bitdefender company (Current)
- KITRI BoB Digital Forensics Mentor (Current)
- Advisor of Cashtree, and Advisor/Investor of Teiren
- Former Senior Security Researcher at LG Vehicle Components
- Former Hallym University Researcher

11 years security experience

15 years software engineer

Pioneered Cyber Peacekeeping Academic Research

Presented @ SecuInside, VXCon, Microsoft Conf, ICDF2C, AIS3 etc.

Organizing committee of ICDF2C and GCC.

HORANGI. A BITDEFENDER COMPANY.



www.linkedin.com/in/kolyaak

Related talks

We ran this workshop first time in Nov 2023 in South Korea and May 2024 in Singapore.

We received the positive feedback from attendees.
So we improve on it and turn it to a talk for Rootcon 2024!



My experience with cloud security

Building in cloud (and securing it) since 2016, it looked totally different then.

Teaching cloud security at BoB for past 3 years.

Started building internal cloud security monitoring 4 years ago.

Using our own product and services.

Ran two TTX in the hybrid environment.

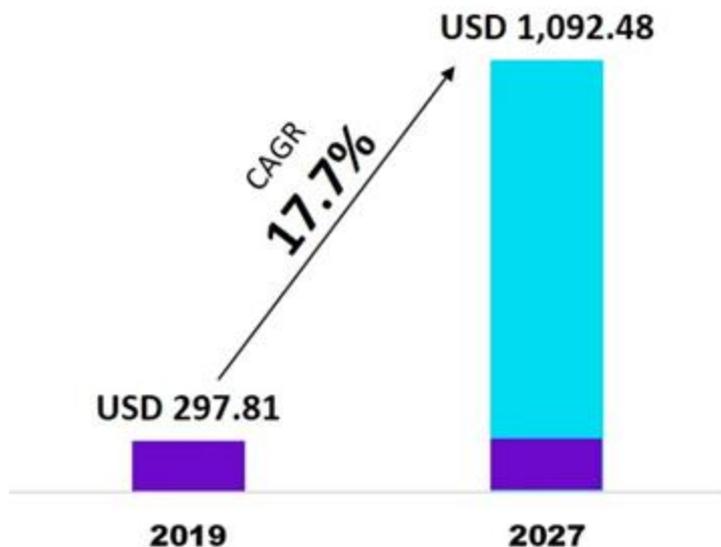
Outline of the presentation

- A quick intro to cloud and cloud security
 - History of cloud breaches
 - Case studies
 - Threat detection in cloud
 - Attack simulation
-

Cloud

Market

Global Cloud Computing Market Size (USD Bn) 2019-2027



- **SaaS** service segment dominated the market by nearly **55%** in 2019
- **Healthcare** segment projected to grow with the fastest CAGR of **18.6%** during 2020 to 2027
- **Asia Pacific** expected to grow with fastest CAGR of **18.5%** during the forecast period

Source: ReportCruX Market Research

Impact of cybersecurity issues



Cost of a breach

The global average cost of a data breach in 2023 was **USD 4.45 million**, a 15% increase over 3 years.

Source: IBM Cost of a Data Breach Report, 2023



Damaging

GoldenEye ransomware inflicted around \$1 billion in damages to its victims.

Source: Bitdefender Business Insights



Scale of the problem

On average, 1 cloud misconfiguration is identified every 20 seconds.

Source: Horangi Threat Report, Covering H1 2023

Detect breach to survive

We live in a norm where it is not “if” but “when” data breach happens.

30,458 security incidents, of which 10,626 were confirmed data breaches in 2024 Data Breach Investigations Report (DBIR) by Verizon.

So, it's paramount to be able to detect a security event and respond to a breach timely.



Cloud Security

Quick Intro

Fundamentals of cloud

On demand resources.

API.

Management plane.

Workloads.

Cloud security

Security of the management plane.

Security of workloads.

Cloud native.

Cloud security

Misconfigurations.

Unmanaged resources - complexity and speed of deployment.

Vulnerabilities in workloads, e.g. instances, Kubernetes, containers.

Vulnerabilities of the platform. The recent vulnerability with AWS ECR.

Threat detection.

Cloud Breaches

History that is a reality

Breaches

2023



AA: recruiting provider



ChatGPT: bug in the code

earlier



Twitter: unpatched vulnerability



Okta: compromised third party service



LastPass: compromised developer's laptop

Cloud breaches

2023



Circle CI



2022



Uber: compromised AWS server.



Pegasus Airlines: misconfigured S3 bucket. 6.5 Terabytes.

earlier



Facebook: exposed AWS server.



Raychat: misconfigured Mongo DB.

No Security is More Expensive



Equifax

- \$700 mln
- 145.5 mln consumers' data

Capital One

- \$100 mln - \$500 mln
- 106 mln consumers' data

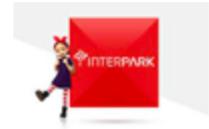


Marriott

- \$124 mln in Europe
- 500 mln user data

Interpark

- 4.5 bln won (\$3.8 million)
- 10 mln users data



Case study

Capital One

Capital One

Using a case study of Capital One breach.

<http://web.mit.edu/smadnick/www/wp/2020-07.pdf>



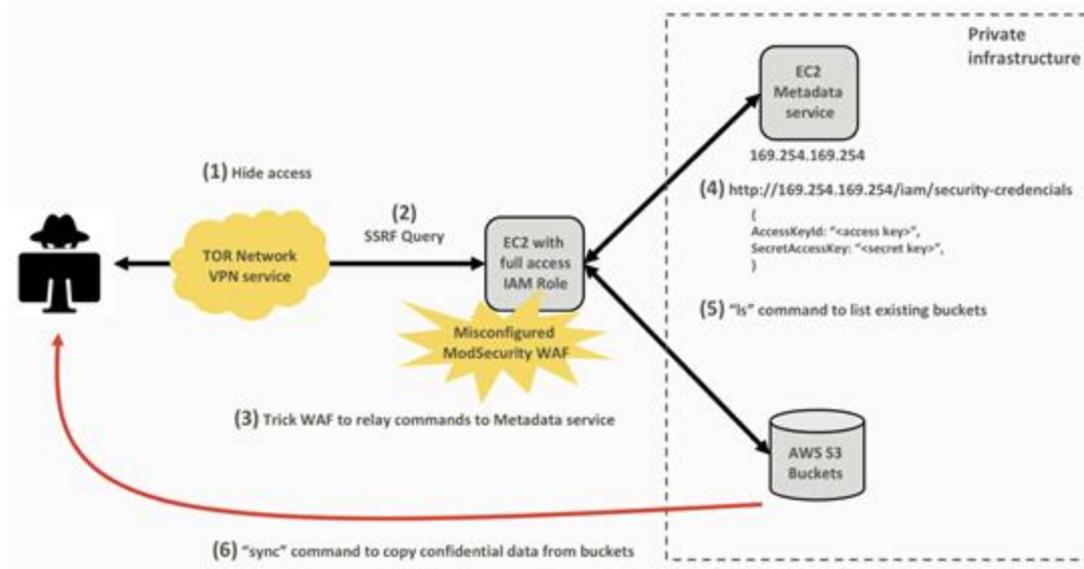
A Case Study of the Capital One Data Breach

Nelson Novaes Neto, Stuart Madnick, Anchises Moraes G. de Paula,
Natasha Malara Borges

Working Paper CISL# 2020-07

January 2020

Anatomy of Capital One attack



Threat Detection in Cloud

Security monitoring

Cloud security alert

splunk>enterprise Apps ▾

Triggered Alerts

Filter App Search & Reporting (search) ▾ Owner All owners ▾ Severity All severity ▾ Alert name All alerts ▾

<input type="checkbox"/>	Time ▾	Alert name ▾	App ▾	Type ▾	Severity ▾
<input type="checkbox"/>	2024-05-23 01:48:26 +08	[CLOUDTRAIL] A bastion instance started	search	Real-time	● Critical
<input type="checkbox"/>	2024-05-23 01:18:34 +08	[CLOUDTRAIL] A bastion instance started	search	Real-time	● Critical

splunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search

index="main" sourcetype="aws:cloudtrail" eventName="StartInstances" dest="1-80cda143bf97c339"

✓ 1 event (01/01970 07:30:00.000 to 23/05/2024 01:48:26.933) No Event Sampling ▾

Events Patterns Statistics Visualization

List ▾ Format 20 Per Page ▾

Time	Event
23/05/2024 01:29:54.000	<pre>{ "action": "us-east-1 eventCategory: Management eventID: b415c789-6934-4ff1-bbea-55a6738ea1e1 eventName: StartInstances eventSource: ec2.amazonaws.com eventTime: 2024-05-22T17:29:54Z eventType: AwsApiCall eventVersion: 1.09 managementEvent: true readOnly: false recipientAccountID: 82797850611 requestID: 334d358e-2ace-4d13-b698-94df6723887b requestParameters: [{}] responseElements: [{}] } sessionCredentialFromConsole: true sourceIPAddress: 132.147.74.225 tags: [{}] userAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 userIdentity: [{}] }</pre>

Show as raw text

host = sincon-splunk | source = s3://aws-cloudtrail-logs-02797785061-3k1246/AWSLogs/02797785061/Cloud... | sourcetype = aws:cloudtrail

Search Analytics Datasets Reports Alerts Dashboards

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the search to a list of people. Click the name to view the alert. Open the alert in Search to...

Alerts

- 1. Suspicious API address
- 2. [CLOUDTRAIL] A bastion instance started

Edit Alert

Trigger Actions

+ Add Actions ▾

When triggered > Add to Triggered Alerts Remove

Send email Remove

To nikityev@bldofender.com

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search. Show CC and BCC.

Priority Highest ▾

Subject [SINCON-LAB] Splunk Alert: 8name

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More ID

Message

```
## Goal
Check the event of the bastion instance started that provides access to sensitive production data.

## Trigger & response
1. Check if the conditions of the launch of the instance are normal.
2. Check who started the instance.
3. If in doubt, verify with the user that he intended to start the instance for the business reason. What is the business reason?
```

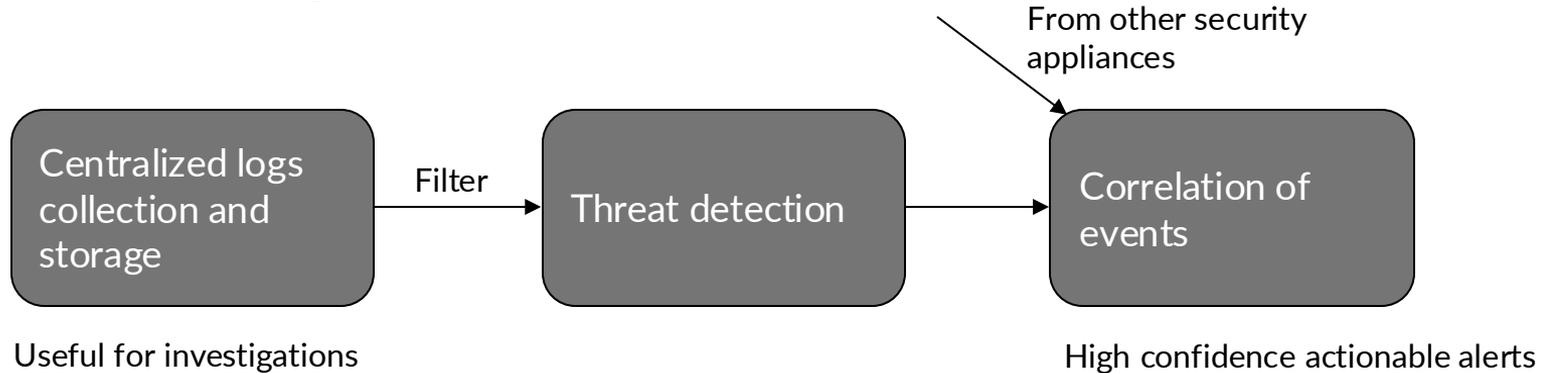
Cancel Save

Detection based on CloudTrail

GuardDuty findings

Splunk alerts

Datadog OOTB detection rules



Quick intro to CloudTrail

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAB8888888888888888",
    "arn": "arn:aws:iam::111111111111:user/alice",
    "accountId": "111111111111",
    "userName": "alice"
  },
  "eventTime": "2020-09-23T09:09:56Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "1.2.3.4",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like G",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home",
    "MobileVersion": "No",
    "MFALused": "No"
  },
  "eventID": "a994a371-9f3a-47d8-575c-5f6ca347281a",
  "eventType": "AwsConsoleSignIn",
  "recipientAccountId": "111111111111"
}
```

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAB8888888888888888",
  "arn": "arn:aws:iam::111111111111:user/alice",
  "accountId": "111111111111",
  "userName": "alice"

  "eventTime": "2020-09-23T09:09:56Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "ConsoleLogin",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "1.2.3.4",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like G
```

<https://www.datadoghq.com/blog/monitoring-cloudtrail-logs/>

Triage

- First quickly confirm whether the security event indicates an incident.
 - Confirm severity.
 - If it's critical, urgently continue the detailed analysis.
 - If it indicates an incident, start the incident response process.
-

Splunk search

New Search
Index= Descriptors | 30,814 events (22/05/2024 02:00:00.000 to 23/05/2024 02:42:45.000) | No Event Sampling

Format Timeline | Zoom Out | Zoom to Selection | Deconstruct

1 Hour per column

Time	Event
23/05/2024 02:42:42.395	2024-05-23T02:42:42.395662+08:00 visit-machine process-agent(1086289): 2024-05-23 02:42:42 +08 PROXESS INFO (gpg/process/runner/runner.go:256 in logCheckDuration) Finish process check #9748 in 11.5118 ms
23/05/2024 02:42:37.000	2024-05-23 02:42:37 +08 CORE INFO (gpg/collector/worker/check_lagger.go:59 in CheckFinished) check-ntp Done running check
23/05/2024 02:42:37.000	2024-05-23 02:42:37 +08 CORE INFO (gpg/collector/worker/check_lagger.go:48 in CheckStarted) check-ntp base-agent
23/05/2024 02:42:37.000	2024-05-23 02:42:37 +08 CORE INFO (gpg/collector/worker/check_lagger.go:59 in CheckFinished) check-ntp base-agent

eventName
#8 | CORE | INFO | (gpg/collector/worker/check_lagger.go:48 in CheckStarted) | check-ntp | Running check...

Aggregations	Raw values
Top values	Top values by time
Events with this field	
Top 10 Values	
Count	%
1108/objects	4,888 29.565%
DescriptorInstancesStatus	1,387 8.232%
getObjact	548 3.335%
DescriptorInstances	432 2.615%
Invoke	311 1.917%
InvokeDetection	219 1.362%

New Search
Index= Descriptors | 83 events (22/05/2024 02:00:00.000 to 23/05/2024 02:37:30.000) | No Event Sampling

Format Timeline | Zoom Out | Zoom to Selection | Deconstruct

1 Hour per column

Time	Event
23/05/2024 02:37:48.000	base-agent: 69-react-1 eventCategory: Management eventID: 69react-1962-14f233b69f6 eventName: DescriberInstances eventSource: HCS-ADMINCON.COM eventTime: 2024-05-22T18:13:48Z eventTimeNormalized: 2024-05-22T18:13:48Z eventVersion: 1.89 managementEvent: true readOnly: true recipientAccountID: 8279780681 responseID: 120af68-956e-923c-822476760482 responseParameters: { [] }

responseParameters: null
sourceIPAccountID: 8279780681
sourceIPAccountIDNormalized: true
sourceIPAddress: 132.147.14.225
sourceIPDetails: { [] }| 23/05/2024 02:37:48.000 | base-agent: 69-react-1 eventCategory: Management eventID: 69react-1962-14f233b69f6 eventName: DescriberInstances eventSource: HCS-ADMINCON.COM eventTime: 2024-05-22T18:13:48Z eventTimeNormalized: 2024-05-22T18:13:48Z eventVersion: 1.89 managementEvent: true readOnly: true recipientAccountID: 8279780681 responseID: 120af68-956e-923c-822476760482 responseParameters: { [] } |

recipientAccountID: 8279780681
responseID: 120af68-956e-923c-822476760482
responseParameters: { [] }| 23/05/2024 02:37:48.000 | base-agent: 69-react-1 eventCategory: Management eventID: 69react-1962-14f233b69f6 eventName: DescriberInstances eventSource: HCS-ADMINCON.COM eventTime: 2024-05-22T18:13:48Z eventTimeNormalized: 2024-05-22T18:13:48Z eventVersion: 1.89 managementEvent: true readOnly: true recipientAccountID: 8279780681 responseID: 120af68-956e-923c-822476760482 responseParameters: { [] } |

recipientAccountID: 8279780681
responseID: 120af68-956e-923c-822476760482
responseParameters: { [] }

Splunk query

- Start with "index=*", set specific date/time range.
 - Select and add fields into the query.
 - By default, parts of the query joint with AND
 - Use AND NOT to filter out noise
 - `index=* AND NOT userAgent="Datadog" AND NOT userAgent="rds.amazonaws.com"`
-

Splunk alerts

The screenshot shows the Splunk Alerts page. At the top, there is a navigation bar with the Splunk logo, 'splunk > enterprise', and 'Apps'. The main navigation menu includes Search, Analytics, Datasets, Reports, Alerts (highlighted), and Dashboards. The top right corner shows user information: Administrator, Messages, Settings, Activity, Help, and a search bar with 'Find'. A 'Search & Reporting' button is also visible.

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

2 Alerts

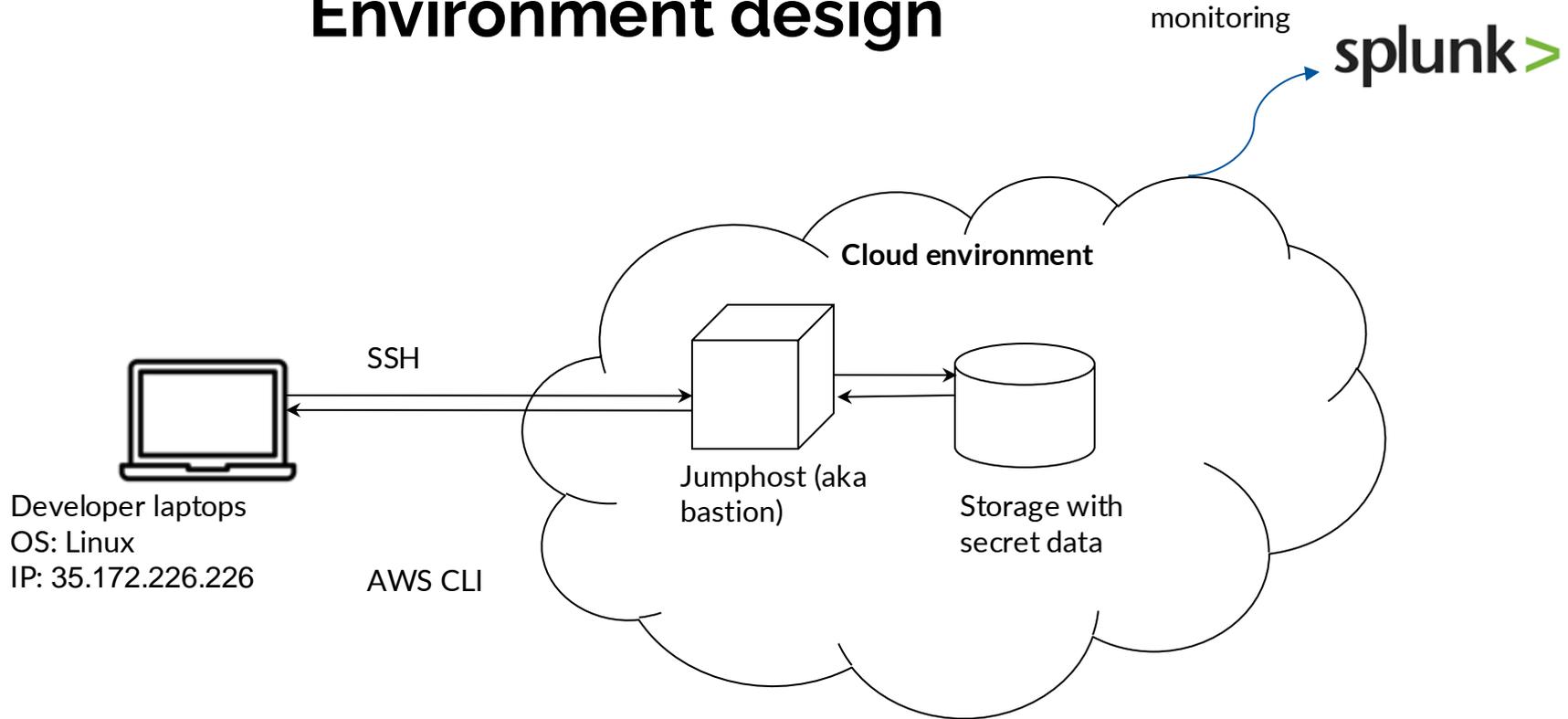
Buttons: All, Yours, This App's, filter [input field] Q

i	Title	Actions	Owner	App	Sharing	Status
>	Suspicious API address	Open in Search Edit	admin	search	Private	Enabled
>	[CLOUDTRAIL] A bastion instance started	Open in Search Edit	admin	search	Global	Enabled

Run cloud attack

Real-world simulation

Environment design



Initial attack vector

- Compromise of the developer laptop

```
ubuntu@victim-machine:~$ sudo ./system-cleaning.sh
Ubuntu cleaner v0.1
Delete backup files...rm: missing operand
Try 'rm --help' for more information.
[OK]
Remove only stale packages...[OK]
Reading package lists... Donetalled packages...
Building dependency tree... Done
Reading state information... Done
[OK]
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
[OK]
Reading package lists... Done..
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
[OK]
Checking the latest Ubuntu updates and run the system update...█
```

Misconfigurations

- Cloud misconfigurations to exploit



Notification and analysis of cloud security alert

Triage

Collection of additional data

Confirmation of the incident

Alert

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk-enterprise' and 'Apps'. Below it, a search bar contains the query: `index="main" sourcetype="aws:cloudtrail" eventName="StartInstances" dest="i-90cda5183bf97c839"`. The search results show 2 events from 01/01/1970 to 23/05/2024. The selected event is from 23/05/2024 at 02:23:08.000. The event details are as follows:

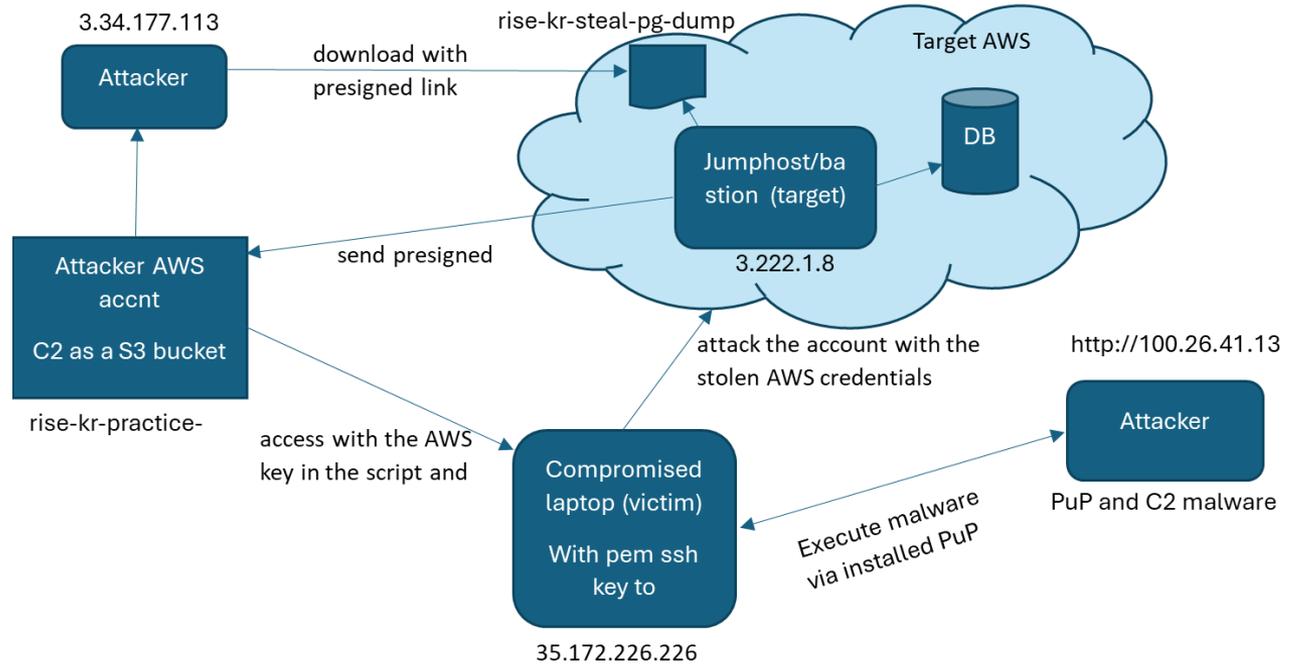
```
{
  "awsRegion": "us-east-1",
  "eventCategory": "Management",
  "eventId": "9f423ac4-226d-45f7-b86d-4ecfba2ffc0b",
  "eventName": "StartInstances",
  "eventSource": "ec2.amazonaws.com",
  "eventTime": "2024-05-22T18:23:08Z",
  "eventType": "AwsApiCall",
  "eventVersion": "1.09",
  "managementEvent": true,
  "readOnly": false,
  "recipientAccountId": "027977850611",
  "requestId": "0578518f-2a45-42be-831c-a8c2a25b7c13",
  "requestParameters": {
    "responseElements": {
      "sourceIpAddress": "35.172.226.226",
      "titleDetails": {
        "userAgent": "aws-cli/2.15.44 Python/3.11.8 Linux/6.8.0-1088-aws exe/x86_64.ubuntu.24 prompt/off command/ec2.start-instances"
      }
    }
  }
}
```

The screenshot shows an email configuration form. It includes fields for 'To' (nakatyeve@bitdefender.com), 'Subject' ([SINCON-LAB] Splunk Alert: \$name), and 'Priority' (Highest). Below these fields, there is a 'Message' section with the following content:

Goal
Check the event of the bastion instance started that provides access to sensitive production data.

Triage & response
1. Check if the conditions of the launch of the instance are normal.
2. Check who started the instance.
3. If in doubt, verify with the user that he intended to start the instance for the business reason. What is the business reason?

Attack flow



Q&A

[https://www.linkedin.com/in/kolyaak/
nakatye@bitdefender.com](https://www.linkedin.com/in/kolyaak/nakatye@bitdefender.com)
