

# 案例分享-某企業AD上百組帳號大量登入失敗導致鎖定事件

- 11月22, 2022



## 某企業AD上百組帳號大量登入失敗導致鎖定事件

### 一、案例故事

某企業客戶於某日下午發生Exchange遭受外部惡意主機大量進行暴力破解攻擊，導致企業內部環境AD伺服器短時間內被鎖定一百多筆帳號事件，而該企業也有在Exchange的WebMail上啟用雙因子認證，這是在短時間內遭受大量暴力破解攻擊，尋求雲智維科技團隊協助。

### 二、解決方案

使用「雲智維資訊顧問代管代維方案」，透過收集客戶單位中各種網路設備syslog、資安設備syslog、Flow及SNMP，從各式數據搭配AI即時分析，從中查找出重要的關鍵數據，找出客戶內部環境網路、資安問題所在。

該企業使用「雲智維資訊顧問代管代維方案」，可從Exchange稽核紀錄中查找登入/登出稽核紀錄，並發現到有大量帳號登入失敗、猜測的紀錄。

服務名稱	登入成功	登出	登入失敗	帳號總數
EXCHANGE	16,713 (46.03%)	16,879 (46.46%)	2,187 (6.02%)	528 (1.43%)
系統	20 (36.46%)	31 (59.62%)	1 (1.92%)	0 (0%)
ONAS	0 (0%)	234 (100%)	0 (0%)	0 (0%)
DC	0 (0%)	3,527 (100%)	0 (0%)	0 (0%)
ERP	4,959 (48.87%)	4,882 (51.10%)	0 (0%)	3 (0.03%)
EIS	1 (50%)	1 (50%)	0 (0%)	0 (0%)
ERP	9 (47.37%)	9 (47.37%)	0 (0%)	1 (5.26%)
ERP	16 (41.03%)	22 (56.41%)	0 (0%)	1 (2.56%)
EXCHANGE_IS	195,409 (100%)	0 (0%)	0 (0%)	0 (0%)
管理	16 (100%)	0 (0%)	0 (0%)	0 (0%)
管理Event log	1 (100%)	0 (0%)	0 (0%)	0 (0%)
系統_IS	8,724 (100%)	0 (0%)	0 (0%)	0 (0%)
系統	1 (25%)	3 (75%)	0 (0%)	0 (0%)

點擊查詢詳細資訊，發現有外部IP使用多個帳號大量嘗試登入、猜測紀錄。

時間	事件	來源 IP	埠	Audit User	來源區域	次數	事件名稱	策略名稱	Policy ID
2022/11/02 14:53:37	Error	152.89.247.188	47914	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	47878	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	47810	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	47848	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	49534	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	48378	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	48590	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	49158	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	48002	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	48004	ad...	DE (德國)	1	audit	ad...	4825
2022/11/02 14:53:37	Error	152.89.247.188	47926	ad...	DE (德國)	1	audit	ad...	4825

藉由統計功能，發現到該IP總共使用了476組帳號進行嘗試

時間	服務	等級	事件	來源 IP	Audit User	次數
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	34	1
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	ch...	1
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	hyf...	1
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	la...	1
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	jo...	1
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	va...	1
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	lu...	1
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	sh...	1
2022/11/02 14:53:37	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	ld7	1
2022/11/02 14:53:35	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	28	1
2022/11/02 14:53:34	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	jas...	1
2022/11/02 14:53:34	EXCHANGE	Error	4825 An account failed to log on (帳戶無法登入) (Login Failure)	152.89.247.188	mar...	1

再藉由客戶所導入的Exchange IIS紀錄中，有發現到外部曾有大量連線到Exchange的「/Autodiscover/Autodiscover.xml」此路徑下

時間	服務	等級	事件	來源 IP	目的 IP	次數
2022/11/02 12:00:00 - 2022/11/02 14:59:53	EXCHANGE_IS	Notice		152.89.247.188	192.168.1.1	1,551
	EXCHANGE_IS	Notice		172.31.1.1	192.168.1.1	723
	EXCHANGE_IS	Notice		123.195.97.138	192.168.1.1	94
	EXCHANGE_IS	Notice		49.217.200.84	192.168.1.1	67
	EXCHANGE_IS	Notice		59.120.221.139	192.168.1.1	63
	EXCHANGE_IS	Notice		111.70.9.11	192.168.1.1	59
	EXCHANGE_IS	Notice		223.137.99.47	192.168.1.1	31
	EXCHANGE_IS	Notice		61.223.80.1	192.168.1.1	23
	EXCHANGE_IS	Notice		111.82.97.107	192.168.1.1	21
	EXCHANGE_IS	Notice		223.141.4.228	192.168.1.1	14
	EXCHANGE_IS	Notice		39.15.2.60	192.168.1.1	12
	EXCHANGE_IS	Notice		111.82.54.31	192.168.1.1	10

查閱相關事件，可得知該路徑「/Autodiscover/Autodiscover.xml」服務，能被有心人士發動Exchange Server觸發對外Autodiscover.\*網域名稱查詢導致帳密遭竊聽外洩。

建議措施:

- 1.啟動聯防封鎖惡意來源攻擊者。
- 2.封鎖企業對Autodiscover.\*網域名稱查詢，以避免內部所有帳密密碼外洩的風險。

漏洞紀錄：<https://www.ithome.com.tw/news/146842>

## 研究人員發現Exchange自動探索配置的瑕疵，並藉此取得近40萬組Windows網域帳密

為了簡化使用者設置收信軟體流程，微軟在Exchange Server提供了「自動探索 (Autodiscover)」功能，但研究人員發現，收信軟體在找尋有關配置檔案的過程裡出現瑕疵，而使得有心人士可能藉由單控特定網域的方式，取得大量使用者帳密

### 三、結論

該企業導入使用「雲智維資訊顧問代管代維方案」，有效解決了企業面臨發生大量暴力破解攻擊時，導致AD網域帳號被鎖定事件時，能夠快速收放問題點所在，給予相關建議並改善，讓企業網路維運與資安安全等級更加提升。

