

如何了解惡意程式感染後對 AD 造成異常設定變動？

前提：近來駭客攻擊鎖定 Active Directory 攻擊的比例升高，攻入 AD 就可加速病毒感染的效率。透過一些駭客工具就可進行帳號提權、進而改變 GPO 限制原則，透過 GPO 大量派送加密勒索病毒，進程式注入攻擊。

因此可透過 Netwrix 來了解是否有嘗試登入(密碼暴力攻擊)活動、異常提權、臨時性帳號活動、GPO 設定的異常變動紀錄，有助於調查不尋常的嘗試登入或可疑設定變動。

本情境適用於: Netwrix for 9.8 及以上版本，監看 Active Directory 模組

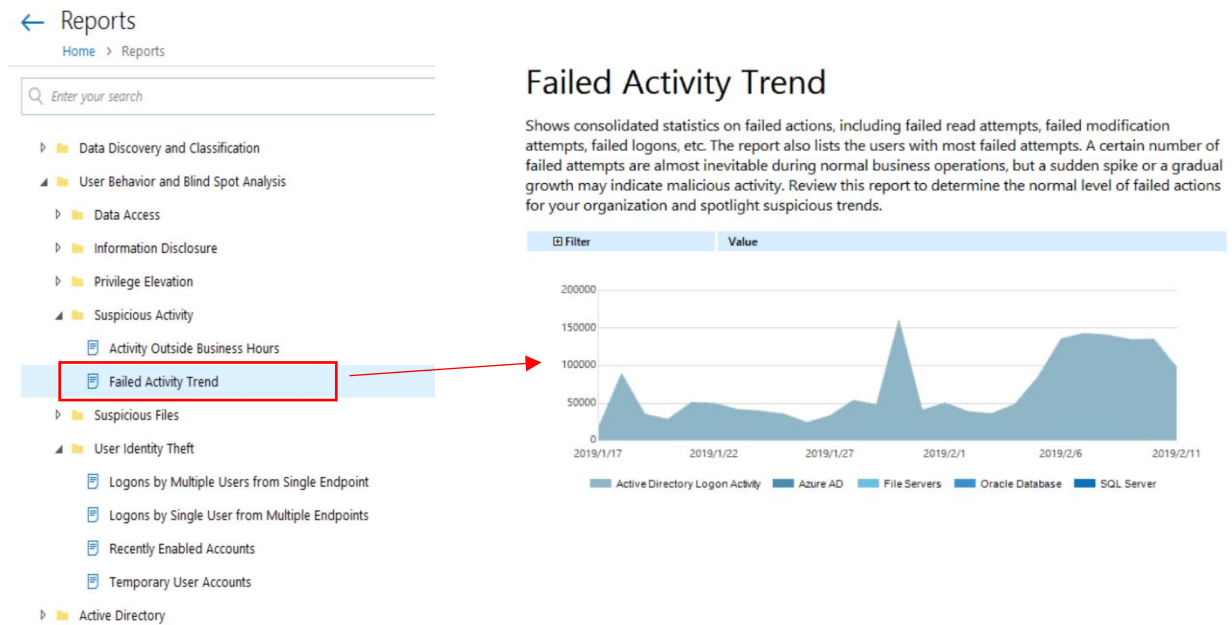
Netwrix 調查範例：



1. 嘗試登入失敗活動檢查

1-1 失敗活動趨勢觀察

報表動線：User Behavior and Blind Spot Analysis→Suspicious Activity → Failed Activity Trend 報表



從該報表過濾條件中 Datasource 點選“ Active Directory Logon Activity” 及想要查找時間區間，就會出現嘗試登入失敗活動趨勢統計圖及人員次數總統計。

1-2 登入失敗活動進階分析

● 分析嘗試登入失敗原因

報表動線：Active Directory → Logon Activity → Failed Logon 報表

← Reports
Home > Reports

Enter your search

- Active Directory
 - Active Directory Changes
 - Active Directory — State-in-Time
 - Group Policy Changes
 - Group Policy — State-in-Time
 - Logon Activity
 - Accounts with Most Logon Activity
 - All Logon Activity
 - Failed Logons**
 - Interactive Logons
 - Successful Logons
 - User Logons and Logoffs on Domain Controllers
- Active Directory Federation Services (AD FS)

Netwrix Auditor Thursday, May 14, 2020 7:20 AM

Failed Logons

Shows failed logon attempts. Use this report to analyze user activity and validate compliance.

Filter	Value
Logon Type	What
Non-Interactive	N/A
Who	Administrator
When	4/15/2020 2:03:17 AM
Where:	dc.nwxdemo.lcl
Workstation:	nwxhost
Cause:	User logon with misspelled or bad password
This entry represents 2 matching events occurring within 600 seconds.	

報表紀錄中會顯示嘗試登入失敗的類型(Logon Type)、時間、帳號、登入 DC 名稱(Where)、使用者電腦名稱(Workstation)、失敗原因...等資訊
從中可觀察到是否有被利用字典檔產生的奇怪帳號或密碼進行嘗試登入活動，及運用程式進行規律性的嘗試登入活動。

● 了解同一帳號是否有多個登入來源電腦

報表動線：User Behavior and Blind Spot Analysis→User Identity Theft → Logons by Single User from Multiple Endpoints 報表

← Reports
Home > Reports

Enter your search

- User Behavior and Blind Spot Analysis
 - Data Access
 - Information Disclosure
 - Privilege Elevation
 - Suspicious Activity
 - Suspicious Files
 - User Identity Theft
 - Logons by Multiple Users from Single Endpoint
 - Logons by Single User from Multiple Endpoints**
 - Recently Enabled Accounts
 - Temporary User Accounts
- Active Directory

Logons by Single User from Multiple Endpoints

Shows users who logged on from several endpoints within a short period of time. Such occurrences may indicate that the account's password was stolen or compromised. Use this report to detect suspicious user activity and prevent data breaches.

Filter	Value
Who:	NWXDEMO\presley (First Attempt: 5/3/2020 12:42:11 AM)
Endpoint	Logon Attempts
desktop.nwxdemo.lcl	1
coach.nwxdemo.lcl	1

2. 提權變動檢查

2-1 檢查管理者群組成員是否有變動

報表動線：Active Directory → Active Directory Changes → Administrative Group Membership Changes 報表

The screenshot shows the Active Directory console on the left with a tree view. The path is: Active Directory > Active Directory Changes > Administrative Group Membership Changes. A red arrow points from this menu item to the report on the right.

Administrative Group Membership Changes

Shows changes to membership of the Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other administrative groups. Members of these groups are entitled to perform critical activities in your IT infrastructure. Subscribe to this report or review it on a regular basis to detect security issues and ensure that administrative group membership is granted or revoked in compliance with your organization's security policies.

Action	Member	Who	When
Removed	nwxdemo.lc\Temp Employees\Elvis Presley	NWXDEMO\atkach	5/13/2020 6:01:36 PM
Where: dc.nwxdemo.lc			
Added	nwxdemo.lc\Europe\Munich\Users\Ludwig Beethoven	NWXDEMO\j.bach	5/14/2020 2:00:00 AM
Where: dc.nwxdemo.lc			

2-2 檢查是否有臨時性帳號變動

報表動線：User Behavior and Blind Spot Analysis → Privilege Elevation → Temporary Users in Privileged Groups 報表

或是

User Behavior and Blind Spot Analysis → User Identity Theft → Recently Enabled Accounts 或 Temporary User Accounts 報表

The screenshot shows the User Behavior and Blind Spot Analysis console on the left with a tree view. The path is: User Behavior and Blind Spot Analysis > Privilege Elevation > Temporary Users in Privileged Groups. A red box highlights this menu item, and a red arrow points from it to the report on the right.

Temporary Users in Privileged Groups

Shows user accounts deleted soon after they were created and added to privileged groups, such as Domain Admins, Enterprise Admins, Schema Admins, Account Operators, and other groups you specified. For each user account, the following is reported: creation and deletion dates and the user who made each change. Use this report to detect intruders attempting to hide malicious activity.

Monitoring Plan: Active Directory Item: Not available,nwxdemo.lc (Domain)

From: 5/13/2020 12:00:01 AM To: 5/14/2020 11:59:59 PM

Timeframe: This year Who Created (Domain\User): %

Who Removed (Domain\User): % Name: %

Group Name: Domain Admins, Enterprise Admins, Sche Existed for (Hours): 5

Sort By: Name

No data found

用來檢查是否有短暫時間內(如 5 小時)的帳號被啟用又很快被停用的行為。

3. GPO 設定變動檢查

3-1 所有 GPO 設定變動檢查

報表動線：Active Directory → Group Policy Changes → All Group Policy Changes 報表 或 Software Restriction Policy Changes 報表

The screenshot displays the Active Directory console with the 'Group Policy Changes' tree on the left. Two items are highlighted with red boxes and arrows pointing to their respective report pages:

- All Group Policy Changes**: This report shows all changes to Group Policy objects, settings, links, and permissions. The table below lists a modification to the 'Default Domain Controllers Policy' by 'NWXDemo\atkach' on 5/13/2020 at 4:39:12 AM.
- Software Restriction Policy Changes**: This report shows changes to the Software Restriction Policies settings. The table below lists a modification to the 'Software Restriction Policy' by 'ENTERPRISE\J.Carter' on 6/30/2016 at 3:18:28 PM, and two removals of file extensions.

Action	What	Who	When
Modified	Default Domain Controllers Policy	NWXDemo\atkach	5/13/2020 4:39:12 AM
Where: dc.nwxdemo.lcl			
Workstation: nwxdemo95.nwxdemo.lcl, nwxdemo96			
Path: General/Details			
Modified: Computer Revisions: 333 (AD), 333 (SYSVOL) -> 335 (AD), 335 (SYSVOL);			

Action	What	Who	When
Modified	Software Restriction Policy	ENTERPRISE\J.Carter	6/30/2016 3:18:28 PM
Where: dc1, enterprise.com			
Path: Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Software Restriction Policies/ Designated File Types/ADE			
Removed	File Extension: BAT; File Type: Windows Batch File;		
Removed	File Extension: EXE; File Type: Application;		

4. 非上班時間的 AD 變動檢查

報表動線：User Behavior and Blind Spot Analysis→Suspicious Activity → Activity Outside Business Hours 報表

The screenshot shows the Netwrix Auditor interface. On the left, a navigation pane lists categories like 'Data Access', 'Information Disclosure', 'Privilege Elevation', and 'Suspicious Activity'. Under 'Suspicious Activity', 'Activity Outside Business Hours' is selected. The main panel shows the report configuration: Monitoring Plan: Active Directory, Item: Not available,nwxdemo.lcl (Domain), From: 5/13/2020 12:00:01 AM, To: 5/14/2020 11:59:59 PM, Timeframe: This month, Hour From: 6 PM, Hour To: 8 AM, Who (Exclude Domain\User): NT AUTHORITY\%, %\$, What: %, Action: Changes,Failed Attempts,Failed Logon, Sort By: Attempts. Below the configuration, the report title 'Activity Outside Business Hours' is displayed, followed by a description: 'Shows users who performed any actions outside their business hours. Use this report to detect suspicious user activity.' A table with columns 'Who' and 'Actions' shows two entries: 'NWXDemo\d.gilmour' with 24 actions and 'NWXDemo\k.kach' with 23 actions. A red circle highlights the '24' value. Below this, a 'Preview Report' section shows the 'Activity by Data Source' report. It includes a table with columns 'Action', 'Object Type', 'What', 'Who', and 'When'. The table shows two entries: 'Modified configuration' for 'dc.nwxdemo.lcl' and 'Modified computer' for 'dc.nwxdemo.lcl'. A red arrow points from the '24' in the first table to the 'Preview Report' section.

Monitoring Plan: Active Directory Item: Not available,nwxdemo.lcl (Domain)

From: 5/13/2020 12:00:01 AM To: 5/14/2020 11:59:59 PM

Timeframe: This month Hour From: 6 PM Hour To: 8 AM

Who (Exclude Domain\User): NT AUTHORITY\%, %\$ What: % Action: Changes,Failed Attempts,Failed Logon Sort By: Attempts

Activity Outside Business Hours

Shows users who performed any actions outside their business hours. Use this report to detect suspicious user activity.

Who	Actions
NWXDemo\d.gilmour	24
NWXDemo\k.kach	23

Activity by Data Source

Shows activity across the entire IT infrastructure, grouped by data source. This report's data set is pre-filtered by the report you reviewed previously.

Action	Object Type	What	Who	When
Modified	configuration	dc.nwxdemo.lcl	NWXDemo\d.gilmour	5/4/2020 3:02:43 AM
Modified	computer	dc.nwxdemo.lcl	NWXDemo\d.gilmour	5/5/2020 3:48:32 AM

設定好非上班時間的時段，並於 DataSource 中點選“ Active Directory” 就會出現非上班時間對 AD Server 產生的變動紀錄。

也可另外運用 Alert 功能設定相關的即時警示 Email 通知：

Netwrix Auditor - VA

Search

Home > Search

Who Action What When Where

Filter Operator Value

Data source Equals Active Directory

Data source Equals Group Policy

Working hours Not equal to From: 8:00:00 AM To: 9:00:00 AM

Specify working hours

From: 8:00:00 AM

To: 5:00:00 PM

Add Cancel

Investigate incidents and

To start browsing your audit data and investigating incidents

Open in new window

SEARCH

Simple mode

Who Object type Action What Where When Details

Who	Object type	Action	What	Where	When	Details
NWXDEMO\j.bach	group	Modified	Security Global Group Member - Added: "nwxdemo.Icl/Europe/Munich/Users/Ludwig Beethoven"	dc.nwxdemo.Icl	5/14/2020 6:00:00 ...	
NWXDEMO\j.bach	group	Modified	Security Global Group Member - Added: "nwxdemo.Icl/Europe/Munich/Users/Ludwig Beethoven"	dc.nwxdemo.Icl	5/14/2020 5:03:25 ...	
NWXDEMO\j.bach	GroupPolicy	Modified	Netwrix_Auditing	dc.nwxdemo.Icl	5/14/2020 5:00:00 ...	
NWXDEMO\j.bach	GroupPolicy	Modified	Default Domain Controllers Policy	dc.nwxdemo.Icl	5/14/2020 4:00:01 ...	
NWXDEMO\DCS	user	Modified	Security Global Group Member - Added: "nwxdemo.Icl/Europe/Munich/Users/Ludwig Beethoven"	dc.nwxdemo.Icl	5/14/2020 3:00:01 ...	

Tools

- Copy search
- Paste search
- Save as report
- Create alert
- Subscribe
- Select columns
- Hide Details
- Export data

設定成“非上班時段的 AD, GPO 設定變動警示通知”

非上班時段的 AD, GPO 設定變動警示通知

Home > All Alerts > 非上班時段的 AD, GPO 設定變動警示通知

General

Recipients

Filters

Thresholds

Risk Score

Response Action

Send alert when the action occurs

On

Name: 非上班時段的 AD, GPO 設定變動警示通知

Description:

Apply tags

Apply tags to the alert to emphasize its importance and to be able to filter similar alerts by their tags.

Tags: Active Directory

Edit