tenable.ad™

LOG4SHELL 與 ACTIVE DIRECTORY：取得網域支配權的五條路徑

白皮書

很多文章報導大篇幅探討了 Log4j 以及此弱點對應用程式 (使用惡名昭彰的 Java 程式庫) 的潛在影響，卻少有人探討攻擊者如何利用此缺陷以最高等級的特殊權限來掌控企業的網域。

大家都會異口同聲地質疑「可是 Active Directory 並沒有使用 Java 呀」...

Active Directory 沒有使用 Java

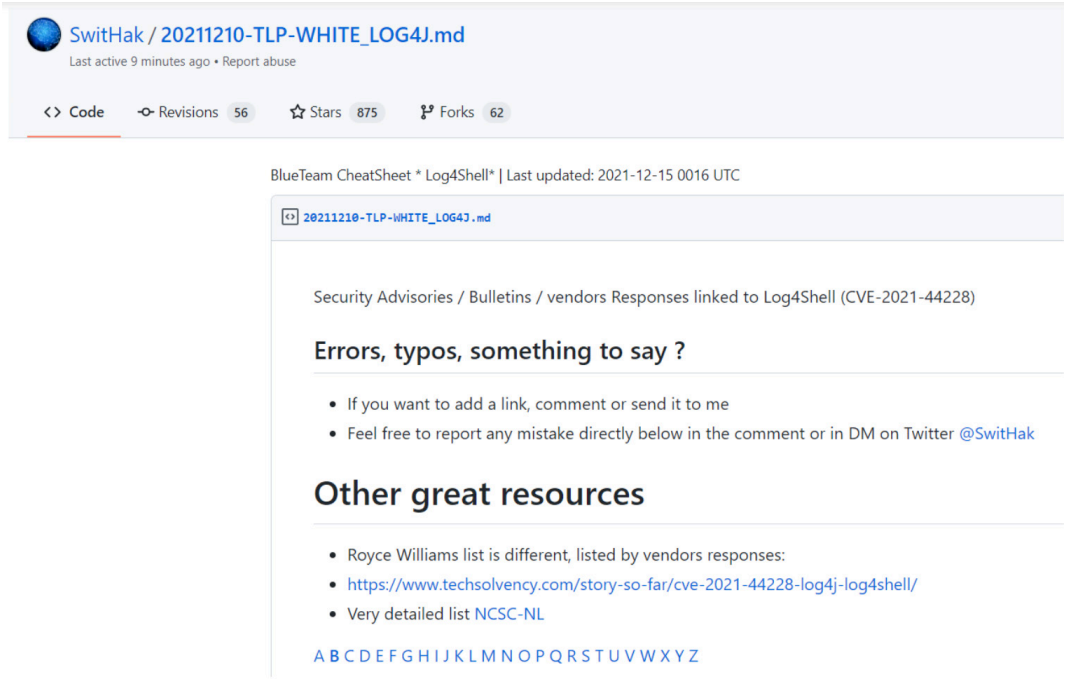
可喜可賀，對吧？某種程度上確實是這樣。然而，事實並不是這麼簡單，儘管這個缺陷並不會直接影響絕大多數的 Active Directory 基礎架構，但卻具有非常實質性的威脅力。

本文為解說方便起見，將假設您熟悉 Active Directory 的使用方式並瞭解其在資訊系統中的策略地位。

我們會探討 Log4Shell 使攻擊者得以透過企業的 Active Directory 基礎架構取得完整網域支配權的五種主要情況。這五種情況並未囊括所有情況，礙於篇幅有限，無法盡數列出，但一定有許多運用類似原理的其他資料外洩途徑。

為數眾多的資料來源試圖一一計算易受 Log4Shell 影響的軟體。雖然這些資料來源無法盡數列出所有軟體，但我們已經盡力運用這些現有的資訊來條列我們的風險概況。

最近一篇提及受到影響的廠商與解決方案的資料載於下列網址：
https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592



- 資料來源：https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

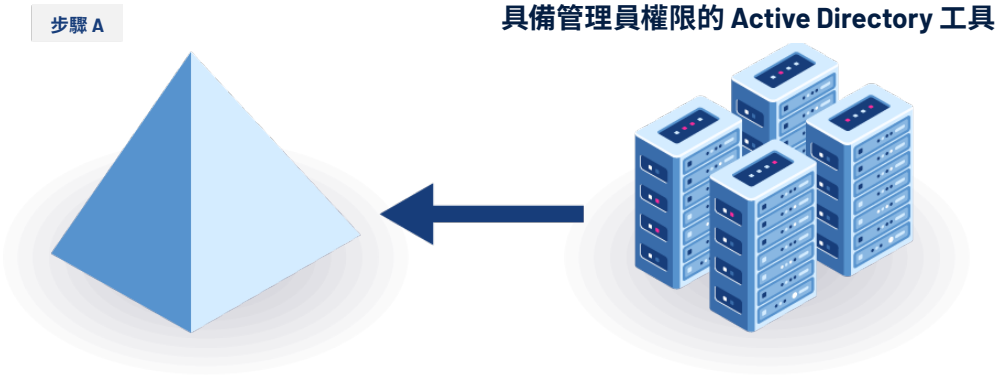
風險情況 #1

易受 Log4Shell 影響的 AD 管理或安全工具 – 影響：網域支配權

Active Directory 的多數解決方案供應商都需要具備權限較高的服務帳戶。這些權限較高的 Active Directory 解決方案能夠對 Active Directory 資料庫和 SYSVOL 目錄執行所有的動作。

如果您正在使用其中一種類型的軟體，而且該軟體受到 Log4j 缺陷的影響，那麼您的區域網路上的任何人 (真的是任何人！) 都可以控制您的 Active Directory。

步驟 1A：運用需要較高權限的 Active Directory 管理或安全軟體：



步驟 1B：Active Directory 管理或安全軟體中的 Log4Shell 缺陷遭到刺探利用：

步驟 1C：Active Directory 網域支配權

這不只是理論上的風險。一項快速搜尋可以找出大量受到 Log4j 影響的 Active Directory 管理軟體。若您有使用這些解決方案中的任何一個，那麼您區域網路上的任何人都可以掌控您的 Active Directory 網域。

風險情況 #2

易受 Log4Shell 影響的 EDR 解決方案 – 影響：網域支配權

即便主流的國家網路安全機構苦口婆心地提出建議，多數 企業仍不斷地在自家的 Active Directory 網域控制器上安裝防毒程式或 EDR 代理程式。這使得他們的攻擊破綻大幅增加，鑄下大錯。

若在網域控制器上安裝 EDR 代理程式，而該代理程式受到這種 Log4Shell 缺陷影響，那麼您區域網路上的任何人都可以掌控您的 Active Directory 網域。

攻擊者也能以另一種方式使用 EDR 解決方案達到相同的效果。即使不使用這個弱點入侵 EDR 代理程式本身，還是可以轉而入侵容易受 Log4Shell 影響的 EDR 管理主控台。若全面掌控 EDR 管理主控台且網域控制器上安裝了 EDR 代理程式，只要簡單按一下就能支配網域。

過度授權或缺乏應用程式開發安全標準

有時候，服務帳戶擁有的權限會超出所需；應用程式產生不當請求、密碼明文顯示在網路上或檔案中；這些問題會引起資料外洩安全疑慮。

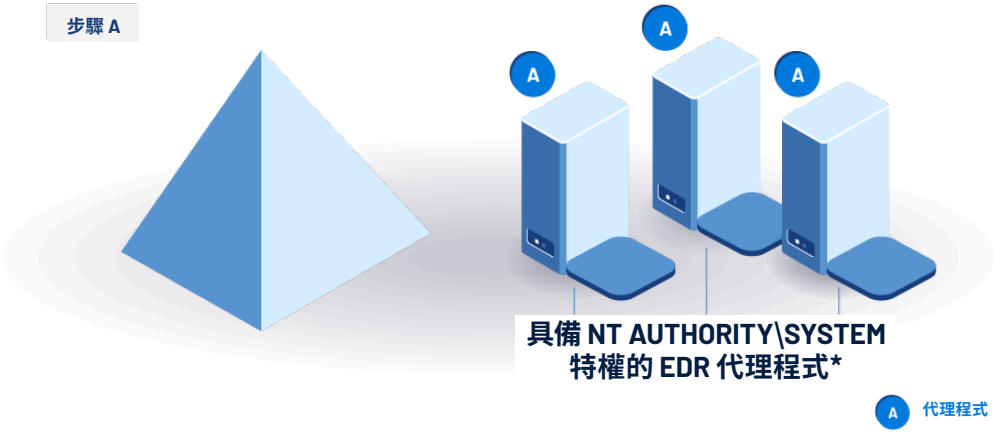
因此，網路控制器不應提供超出目錄運作所需的服務，以防電腦的攻擊破綻擴大。

R10 - 第一要務

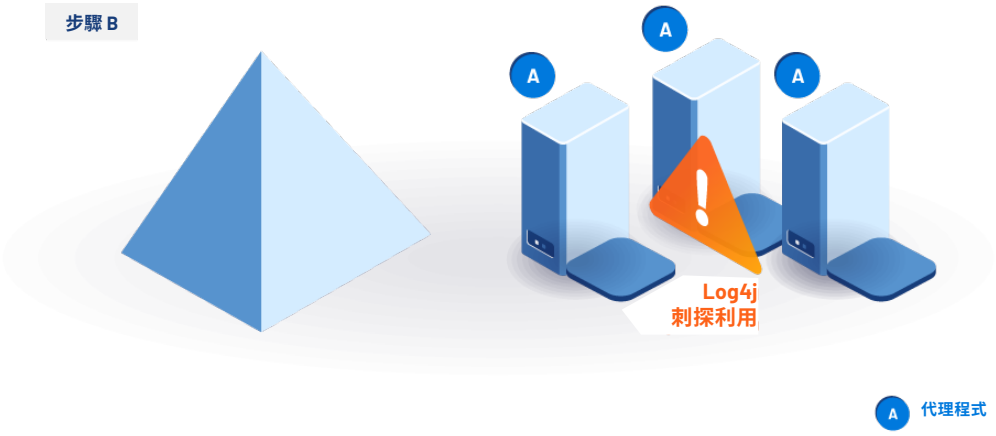
務須注意，防毒軟體是一種應用程式。所以軟體缺陷可能會遭有心人士刺探利用，進而入侵電腦。在重要的伺服器 (如 DC) 上安裝防毒軟體會增加攻擊破綻。因此不建議在網域控制器上安裝軟體 (防毒軟體、備份或清查代理程式等)。
如果符合下列條件，不妨使用 DC 的監控解決方案：
- 建置 DC 專用的監控基礎架構
- 使用解決方案專用的服務帳戶
- 不要在 DC 上安裝偵聽代理程式
- 使用由值得信賴的廠商研發的工具

- 資料來源：https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf

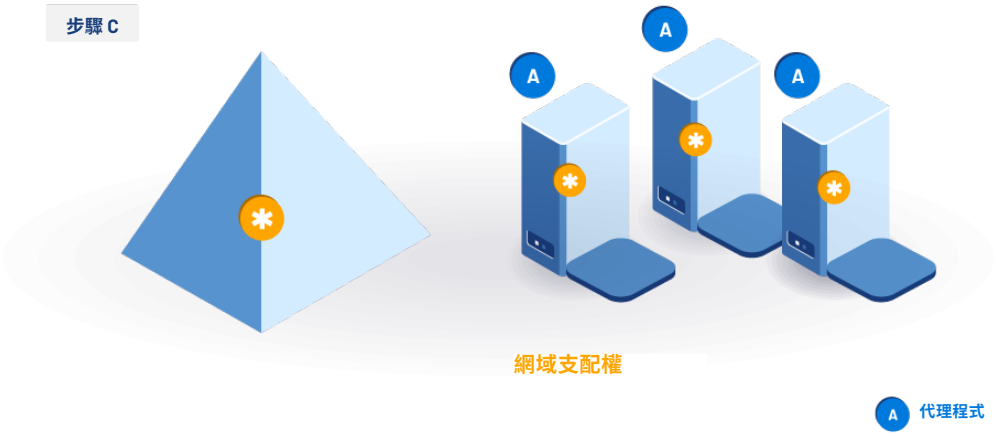
步驟 2A：在企業的網域控制器上安裝 EDR 代理程式：



步驟 2B：Active Directory 網域控制器上安裝的 EDR 代理程式中的 Log4Shell 遭到刺探利用：



步驟 2C：Active Directory 網域支配權：



再次重申，許多 EDR 供應商都發現他們的內部部署管理主控台受到 Log4Shell 影響：如果您使用的是這類 EDR，那麼您區域網路上的任何人都可以掌控您的 Active Directory 網域。

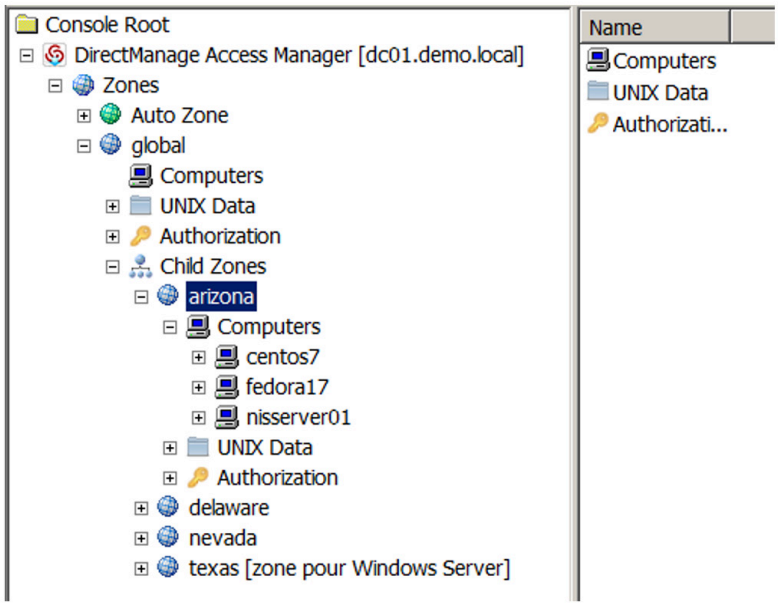
風險情況 #3

有些 Linux/Unix 系統處於「AD 橋接」狀態，而且安裝了易受 Log4Shell 影響的應用程式或程式 – 影響：TIER-1 資料外洩

Active Directory 橋接 (AD 橋接) 是一種可讓使用者透過 Active Directory 連線識別碼與非 Windows 系統 (Unix、Linux、MacOS) 連線的機制。這種架構使系統管理員只要使用一種目錄服務 (Active Directory) 就能輕鬆管理使用者、應用程式、資料及網路的其他部分。

使用某些 Linux 發行版本的原生功能或使用功能更多樣化的商用產品可建置 AD 橋接功能。請注意，Linux/Unix 伺服器電腦在 Microsoft 階層處理模式中通常被視為 Tier-1。

Unix 和 Windows 兩方生產團隊之間的管理習慣差異甚大。沒有哪一方比較好或比較差，純粹只是不同。其中一個差異可從 AD 橋接設計看出，使用 Unix 電腦時，服務帳戶的密碼需與整組 Unix Tier-1 電腦相同。所以如果其中一台 Unix 電腦遭到入侵，攻擊者會提升自己的本機權限並橫向移至全部的 Tier-1 電腦。



- 資料來源：https://www.identitycosmos.com/http:/www.identitycosmos.com/technique/unix_nis_maps_active-directory

步驟 3A：建置 AD 橋接：Unix 系統與 Active Directory 整合在一起並透過 Kerberos 整合安裝應用程式

步驟 3B：Unix 系統或透過 Kerberos 整合的應用程式上的 Log4Shell 缺陷遭到刺探利用：

步驟 3C：Unix 系統遭到入侵，可能會橫向移動至 Tier-1 電腦的所有 UNIX 系統。

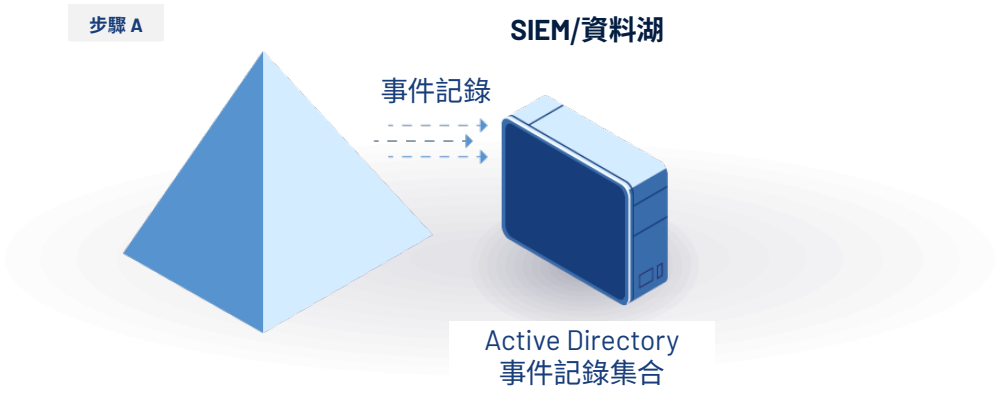
風險情況 #4

易受 Log4Shell 影響的 SIEM 或資料湖解決方案 – 影響：顯而易見

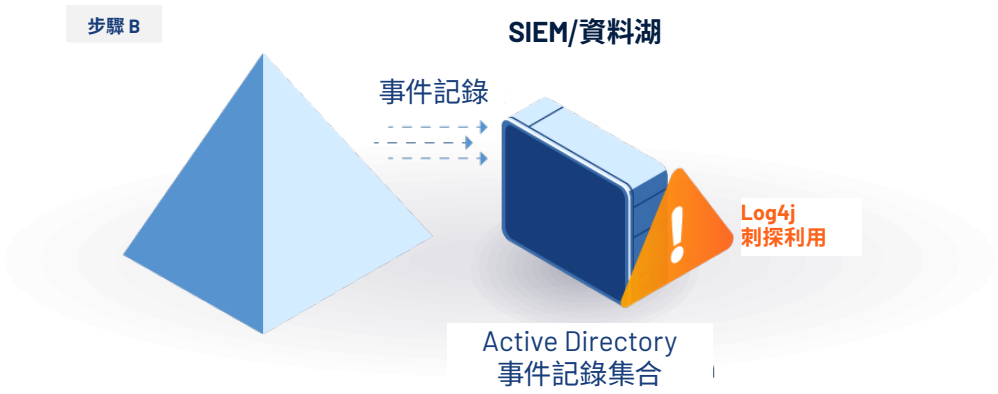
多數企業都會使用 SIEM 和/或資料湖解決方案來收集、存放與關聯資安事件。

如果 SIEM 或資料湖解決方案易受 Log4Shell 的影響，攻擊者可以操控收集而來的資料或變更 SIEM 內的警示組態以隱藏他們在 Active Directory 內的舉動。

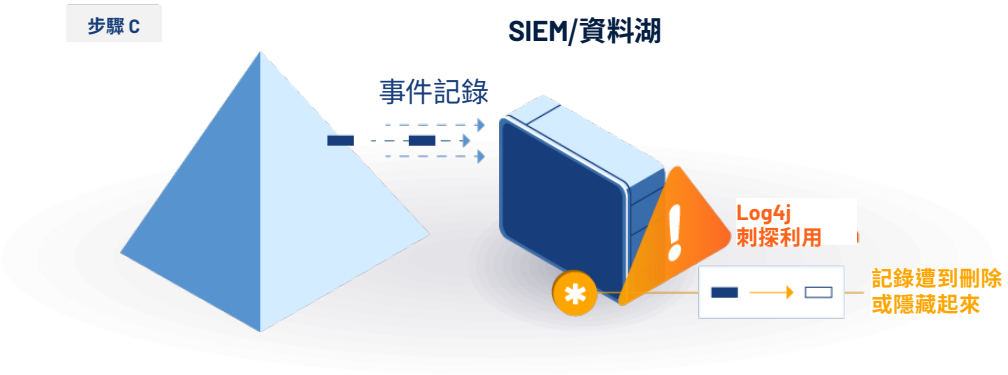
步驟 4A：使用網域控制器的事件集合來建置 SIEM



步驟 4B：SIEM 上的 Log4Shell 缺陷遭到刺探利用。



步驟 4C：攻擊者的處理能力足以刪除 SIEM 中的某些資料或修改相互關聯或事件警示規則，藉此隱藏在 Active Directory 中建立的所有惡意操作。



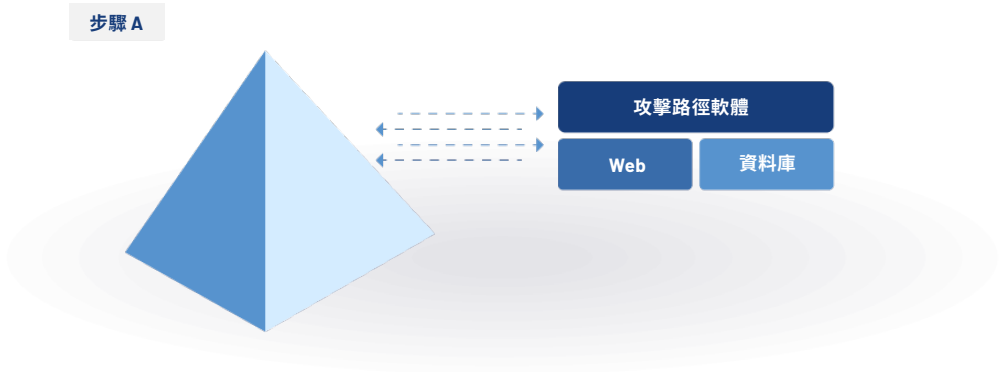
風險情況 #5

易受 Log4Shell 影響的 AD 路徑視覺化呈現解決方案 – 影響：後門程式隱藏

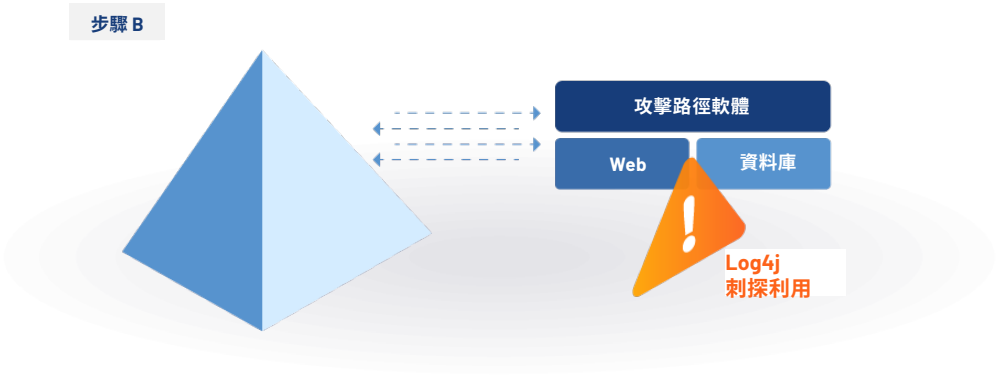
Log4Shell 缺陷有個特點：它可以影響軟體本身，也可以只影響其中的某個元件。這使得清查此缺陷的工作變得極為複雜，因為企業必須能夠掃描和稽查所有元件，而不只是軟體「表面」。

其中一個例證是某些以開放原始碼程式庫為基礎的攻擊路徑視覺化呈現解決方案會受到 Log4Shell 缺陷影響。

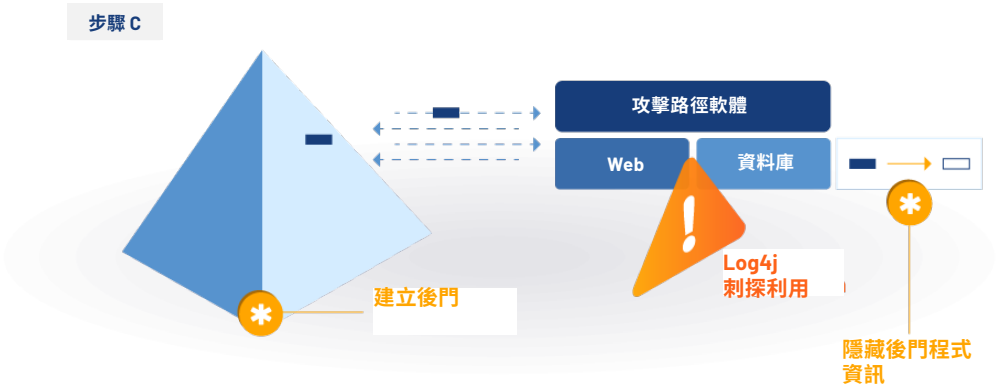
步驟 5A：使用網域控制器中的資訊集合來建置攻擊路徑視覺化呈現解決方案。



步驟 5B：Active Directory 攻擊路徑視覺化呈現軟體其中一個元件上的 Log4Shell 缺陷遭到刺探利用。



步驟 5C：此時攻擊者可利用 Active Directory 的錯誤設定 (通常是為了透過後門程式不斷地進出 AD)，同時隱匿自己的一切惡意操作，不讓攻擊路徑視覺化呈現工具的使用者發現。

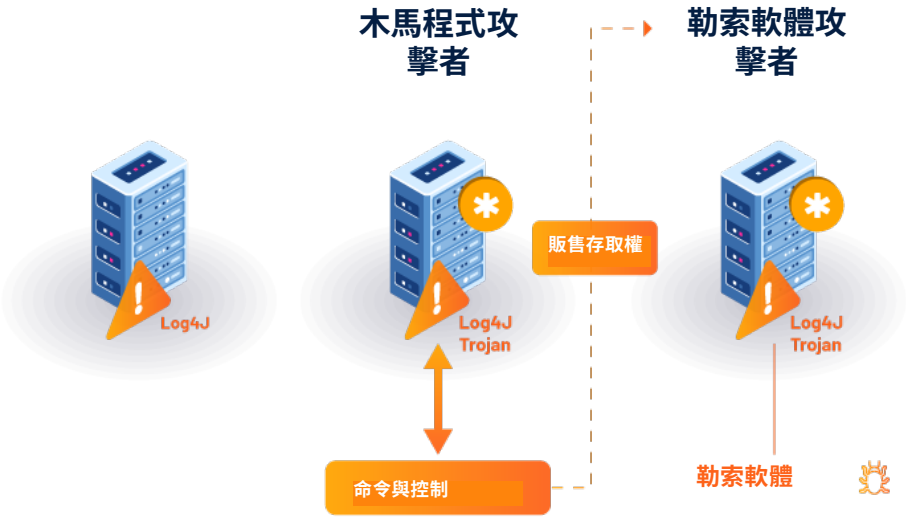


絕大多數的攻擊路徑/資料視覺化呈現解決方案都會使用 Neo4j 來存放 AD 資料。截至本文撰文當日，Neo4j 4.2 以上的版本仍受到 Log4Shell 缺陷所影響。下例十分貼切地說明了分層結構相依關係的重要性，特別是對開放原始碼程式而言。

- 資料來源：https://community.neo4j.com/t/log4j-cve-mitigation-for-neo4j/48856

Log4Shell 缺陷會被勒索軟體攻擊者刺探利用嗎？

一般而言，新弱點不會立刻遭到勒索軟體刺探利用。其他的攻擊者則可能會立即利用。例如，「初次感染」後轉售存取權以及透過木馬程式在「命令與控制」模式下進行遙控的威脅執行者最有可能利用像 Log4Shell 這樣的新弱點趁虛而入：



也就是說，Log4Shell 這個弱點僅僅問世 5 天後就遭到新型的勒索軟體大舉刺探利用。這種新型勒索軟體「Khonsari」利用 Log4Shell 部署網路搜尋工具，藉由這種方式部署加密承載。勒索軟體典型的漸進式手法。

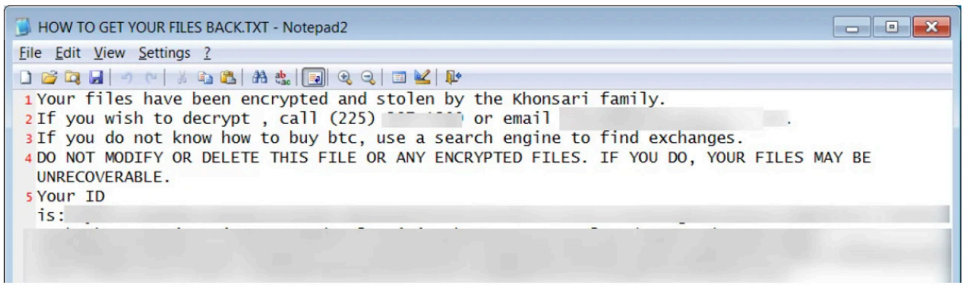
First Log4j exploit installing ransomware

Yesterday, BitDefender reported that they found the first ransomware family being installed directly via Log4Shell exploits.

The exploit downloads a Java class from `hxxp://3.145.115[.]94/Main.class` that is loaded and executed by the Log4j application.

Once loaded, it would download a .NET binary from the same server to install new ransomware [VirusTotal] named 'Khonsari.'

This same name is also used as a the extension for encrypted files and in the ransom note, as shown below.



- 資料來源：https://www.bleepingcomputer.com/news/security/new-ransomware-now-being-deployed-in-log4shell-attacks/

總結

如果 Active Directory 對貴公司很重要 (但願如此)，那麼您迫切需要針對本文中特別提出的所有類型的解決方案加強 Log4J 掃描和修復措施。所有這些解決方案都有可能將貴公司的直接或間接 AD 控制權交給攻擊者。

如需 Log4Shell 的更多相關資訊，請參閱 Tenable 網站上的下列文章：

https://zh-tw.tenable.com/blog/apache-log4j-flaw-a-fukushima-moment-for-the-cybersecurity-industry

https://zh-tw.tenable.com/blog/apache-log4j-flaw-puts-third-party-software-in-the-spotlight

https://zh-tw.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability

為了在不提升權限的情況下，使用無代理程式的解決方案保障貴公司 Active Directory 基礎架構的安全，請參閱我們網站上的 Tenable.ad 專區：https://zh-tw.tenable.com/products/tenable-ad

感謝您撥冗閱覽本文。
Tenable 安全策略師 Sylvain Cortes

關於 Tenable

Tenable, Inc. 是一家 Cyber Exposure 分析公司。全球超過有 30,000 家企業仰賴 Tenable 協助瞭解並降低網路風險。身為 Nessus 的創造者，Tenable 拓展了自己在弱點方面的專業知識，以提供全球第一個可在任何運算平台上查看和維護任何數位資產安全的平台。在 Tenable 的客戶中，包含超過 50% 的財星 500 大企業、超過 30% 的全球 2000 大企業以及大型政府機構。如需深入瞭解，請前往 zh-tw.tenable.com。

tenable.ad