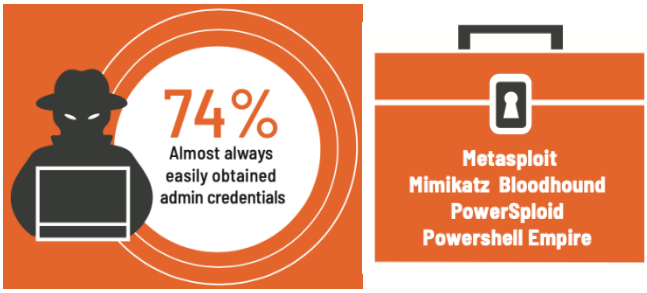
Attivo
NETWORKS®

เราจะสามารถปกป้อง Active Directory สำคัญในองค์กรอย่างไร?

Active Directory (AD) เป็นเซอร์วิสที่บริษัท Microsoft ใช้เป็นเครื่องมือในการบริหารจัดการผู้ใช้งาน โดยการกำหนดนโยบาย (Group Policy Object หรือ GPO) การเข้าถึงทรัพยากรต่าง ๆ ในเครือข่ายของระบบปฏิบัติการ Windows OS ทั้งนี้ Active Directory ถูกออกแบบมาเพื่อเข้ามาช่วยบริหารจัดการผู้ใช้งานและแลกเปลี่ยนข้อมูลในกลุ่มสมาชิกที่อยู่ภายใต้ Active Directory ที่อยู่ใน Domain เดียวกัน

ถ้าหากมีผู้ไม่ประสงค์ดี ทำการโจมตีและยึดเครื่องภายในองค์กรได้สำเร็จ และเครื่องที่ถูกโจมตีมีการเชื่อมต่อกับ Active Directory จะทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลบน Active Directory ได้ทันทีและยากต่อผู้ดูแลระบบที่จะตรวจจับการโจมตีที่เกิดขึ้น เพราะเครื่องที่เชื่อมต่อกับ Active Directory ทุกเครื่องจะมีสิทธิ์สามารถเข้าไป “อ่าน” ข้อมูลใน Active Directory ได้ทั้งหมด จึงทำให้การโจมตีนี้เป็นการเข้าใจว่าเป็นพฤติกรรมปกติ และทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูล ไม่ว่าจะเป็น User Accounts, System Accounts และ Domain Members เป็นต้น ร่วมไปถึงยังสามารถตรวจสอบการใช้งานของผู้ใช้งานที่อยู่ใน Active Directory หรือเข้าถึง Privileged Accounts บน Active Directory เพื่อเข้าไปยังระบบอื่นที่มีข้อมูลสำคัญ เช่น Trusted Domain Controllers, Database Server เป็น โดย Attivo Networks นำเสนอ ADSecure ที่เป็นส่วนหนึ่งของ Attivo Networks ThreatDefend™ Detection Platform ในการป้องกันการเข้าถึงและโจมตี Active Directory



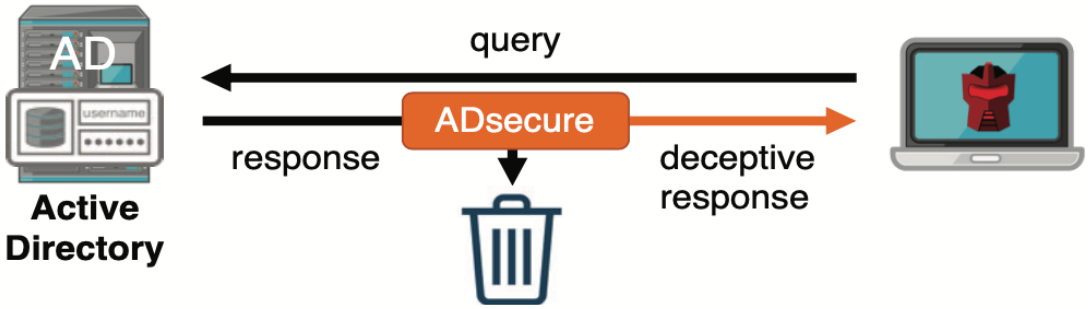
รูปที่ 1. สถิติการโจมตี Privileged Account ในปัจจุบัน

ปกป้อง Active Directory (AD) ที่มีข้อมูลสำคัญที่สุดในองค์กรด้วย

ตรวจจับ AD Queries **ปกป้องข้อมูลจริง** **เบี่ยงเบนข้อมูลไปกับดัก** **รวบรวมข้อมูล TTPs**

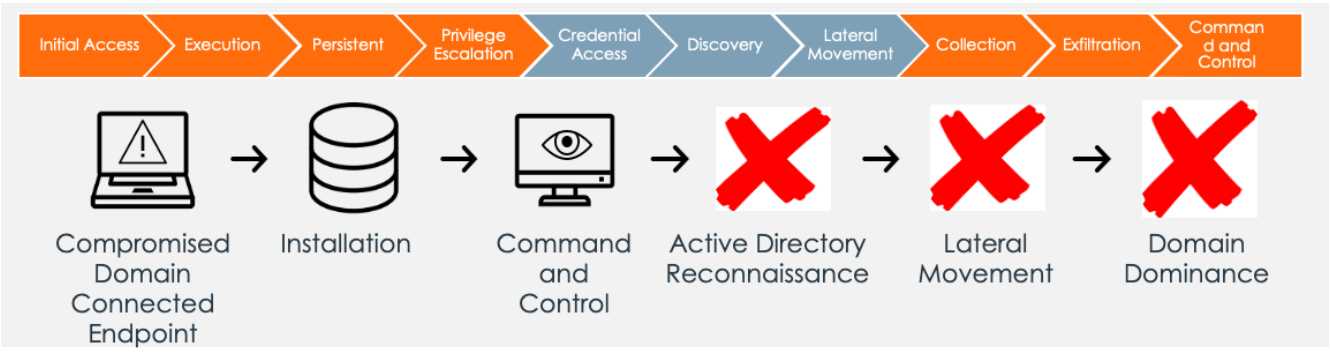
ADSecure

ADSecure เป็น Feature หนึ่งของ ThreatDefend™ Detection Platform ออกแบบมาเพื่อป้องกันการโจมตี Active Directory โดยเฉพาะ โดยทำการสร้าง Deceptive Credentials ด้วยการเข้าไปศึกษาข้อมูลที่อยู่ภายใน Active Directory หลังจากทำการศึกษาข้อมูลเสร็จ จะทำการสร้าง Active Directory Infrastructure ที่เปรียบเสมือน Production Active Directory แต่ทำหน้าที่เป็นกับดักหรือเหยื่อล่อในมุมมองของผู้โจมตี และทำการส่งข้อมูลปลอมทั้งหมดไปเก็บไว้ที่เครื่องของผู้ใช้งานทุก ๆ เครื่องที่ได้ทำการติดตั้ง Agent หากมีผู้ไม่ประสงค์ดีทำการ query ข้อมูล ที่ Active Directory จากเครื่องที่ไม่ได้รับอนุญาตจะมีการตอบกลับด้วยข้อมูล Deceptive Credentials ดังกล่าว รวมไปถึงการหลบซ่อนข้อมูลจริงที่อยู่ภายในระบบ Active Directory ในขณะเดียวกันก็ทำการเก็บข้อมูลการใช้งานต่าง ๆ ที่เกิดขึ้นเพื่อใช้ในการตรวจสอบและแจ้งเตือนผู้ดูแลระบบต่อไป



รูปที่ 2 รูปแบบการทำงานของ AD Secure

ทั้งนี้ ADSecure ยังสามารถเข้ามาช่วยแก้ไขปัญหาในการเกิด Lateral Movement ภายในองค์กรได้อย่างทันท่วงที โดยทำการสร้างข้อมูลปลอมหรือ Deception Credentials และเบี่ยงเบนเป้าหมายการเข้าถึงข้อมูลดังกล่าว ไปยัง Deception Platforms เพื่อใช้ในการวิเคราะห์ การเฝ้าระวัง การตรวจจับ และผู้บุกรุกได้



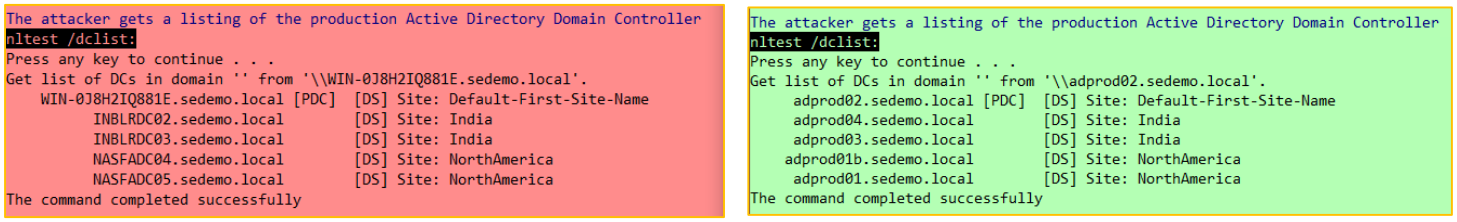
รูปที่ 3 รูปแบบการโจมตีในปัจจุบัน

ตัวอย่างการทำงานเปรียบเทียบ

สีแดง คือ Endpoint ที่ไม่มีการใช้งาน ADSecure และ สีเขียว คือ Endpoint ที่เปิดใช้งาน ADSecure

รูปภาพที่ 5 ทางด้านซ้ายมือแสดงการใช้งานคำสั่ง nltest/dclist ตามด้วย Domain ขององค์กร เมื่อกดคำสั่งดังกล่าวจะแสดงผลโดยจะมีข้อมูล Domain Controller ที่มีอยู่ใน Domain ขององค์กร และ Domain Controller อยู่ที่เครื่องของผู้ใช้งาน

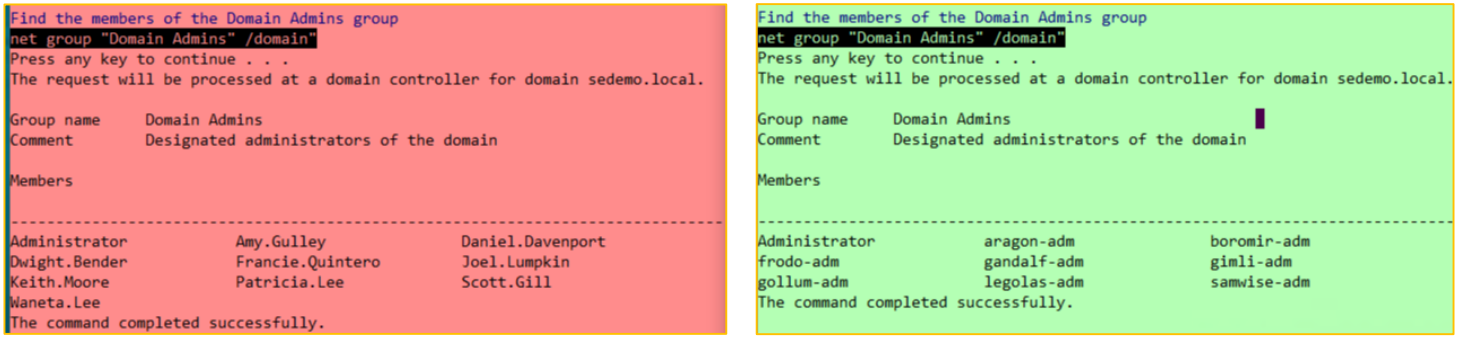
รูปภาพที่ 5 ทางด้านขวามือแสดงการใช้งานคำสั่ง nltest/dclist ตามด้วย Domain ขององค์กรเมื่อกดคำสั่งดังกล่าวจะแสดงผลโดยจะมีข้อมูล Domain Controller ที่มีอยู่ใน Domain ขององค์กร**ที่ถูกปลอมแปลงโดย Attivo Networks** และข้อมูล Domain Controller ที่อยู่ที่เครื่องของผู้ใช้งาน**ที่ถูกปลอมแปลงโดย Attivo Networks เช่นเดียวกัน**



รูปภาพที่ 5 แสดงถึงการ ใช้คำสั่ง nltest /dclist:

รูปภาพที่ 6 ทางด้านซ้ายมือแสดงถึงการใช้คำสั่ง net group “Domain Admins” /domain ซึ่งแสดงข้อมูล Domain Administrator ที่มีใน Domain ขององค์กร

รูปภาพที่ 6 ทางด้านซ้ายมือแสดงถึงการใช้คำสั่ง net group “Domain Admins” /domain ซึ่งแสดงข้อมูล Domain Administrator ที่มีใน Domain **ที่ถูกปลอมแปลงโดย Attivo Networks**



รูปภาพที่ 6 Net Group “Domain Admins” /domain

ถ้าสนใจให้เข้าไปนำเสนอหรือต้องการข้อมูลเพิ่มเติมติดต่อได้ที่

Nattapong@i-secure.co.th หรือ 099-239-6289