

Attivo Networks.
All rights reserved

The logo features the word "Attivo" in a large, white, sans-serif font with a stylized arrowhead pointing left from the 'A'. Below it, the word "NETWORKS" is written in a smaller, white, all-caps, spaced-out sans-serif font, followed by a registered trademark symbol (®). The background is a solid orange color with a faint, glowing network of white lines and nodes overlaid on a world map.

Attivo

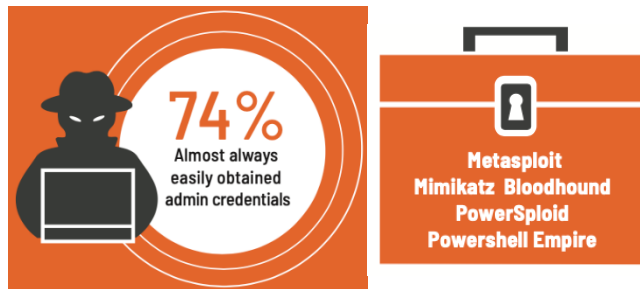
NETWORKS®

Attivo Networks and BOT sink are registered trademarks of Attivo Networks, Inc.

เราจะสามารถปกป้อง Active Directory สำคัญในองค์กรอย่างไร?

Active Directory (AD) เป็นเซิร์ฟเวอร์ที่บริษัท Microsoft ใช้เป็นเครื่องมือในการบริหารจัดการการใช้งาน โดยการกำหนดนโยบาย (Group Policy Object หรือ GPO) การเข้าถึงทรัพยากรต่าง ๆ ในเครือข่ายของระบบปฏิบัติการ Windows OS ทั้งนี้ Active Directory ถูกออกแบบมาเพื่อเข้ามาช่วยบริหารจัดการการใช้งานและแลกเปลี่ยนข้อมูลในกลุ่มสมาชิกที่อยู่ภายใต้ 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 รวมไปถึงยังสามารถตรวจสอบการใช้งานของผู้ใช้งานที่อยู่ใน Active Directory หรือเข้าถึง Privileged Accounts บน Active Directory เพื่อเข้าไปยังระบบอื่นที่มีข้อมูลสำคัญ เช่น Trusted Domain Controllers, Database Server เป็นต้น 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

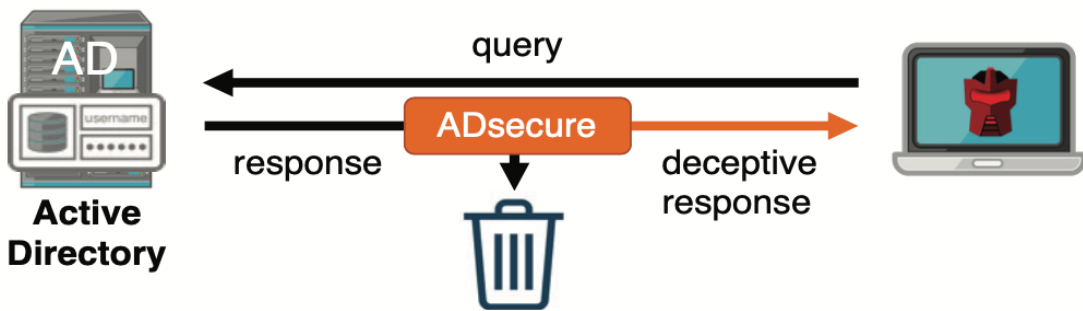


เบี่ยงเบนข้อมูลไปกับดัก



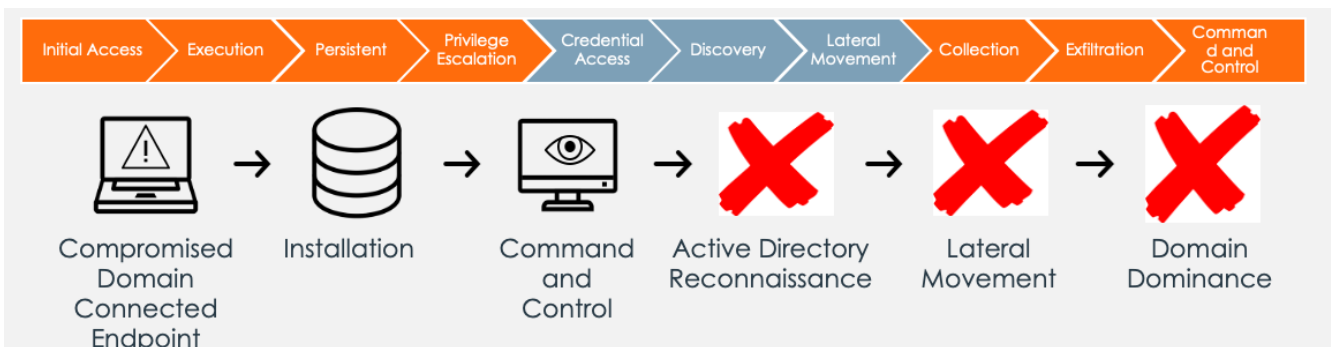
รวบรวมข้อมูล TTPs

ADSecure 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 nlttest/dclist ตามด้วย Domain ขององค์กร เมื่อกรอกคำสั่งดังกล่าวจะแสดงผลโดยจะมีข้อมูล Domain Controller ที่มีอยู่ใน Domain ขององค์กร และ Domain Controller อยู่ที่เครื่องของผู้ใช้งาน

รูปภาพที่ 5 ทางด้านขวามือแสดงการใช้งานคำสั่ง nlttest/dclist ตามด้วย Domain ขององค์กรเมื่อกรอกคำสั่งดังกล่าวจะแสดงผลโดยจะมีข้อมูล Domain Controller ที่มีอยู่ใน Domain ขององค์กรที่ถูกปลอมแปลงโดย Attivo Networks และข้อมูล Domain Controller ที่อยู่ที่เครื่องของผู้ใช้งานที่ถูกปลอมแปลงโดย Attivo Networks เช่นเดียวกัน

```
The attacker gets a listing of the production Active Directory Domain Controller
nlttest /dclist:
Press any key to continue . . .
Get list of DCs in domain '' from '\\WIN-0J8H2IQ881E.sedemo.local'.
WIN-0J8H2IQ881E.sedemo.local [PDC] [DS] Site: Default-First-Site-Name
INBLRDC02.sedemo.local [DS] Site: India
INBLRDC03.sedemo.local [DS] Site: India
NASFADC04.sedemo.local [DS] Site: NorthAmerica
NASFADC05.sedemo.local [DS] Site: NorthAmerica
The command completed successfully
```

```
The attacker gets a listing of the production Active Directory Domain Controller
nlttest /dclist:
Press any key to continue . . .
Get list of DCs in domain '' from '\\adprod02.sedemo.local'.
adprod02.sedemo.local [PDC] [DS] Site: Default-First-Site-Name
adprod04.sedemo.local [DS] Site: India
adprod03.sedemo.local [DS] Site: India
adprod01b.sedemo.local [DS] Site: NorthAmerica
adprod01.sedemo.local [DS] Site: NorthAmerica
The command completed successfully
```

รูปภาพที่ 5 แสดงถึงการ ใช้คำสั่ง nlttest /dclist:

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

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

```
Find the members of the Domain Admins group
net group "Domain Admins" /domain
Press any key to continue . . .
The request will be processed at a domain controller for domain sedemo.local.

Group name      Domain Admins
Comment         Designated administrators of the domain

Members

-----
Administrator   Amy.Gulley      Daniel.Davenport
Dwight.Bender   Francie.Quintero Joel.Lumpkin
Keith.Moore     Patricia.Lee    Scott.Gill
Waneta.Lee

The command completed successfully.
```

```
Find the members of the Domain Admins group
net group "Domain Admins" /domain
Press any key to continue . . .
The request will be processed at a domain controller for domain sedemo.local.

Group name      Domain Admins
Comment         Designated administrators of the domain

Members

-----
Administrator   aragon-adm     boromir-adm
frodo-adm       gandalf-adm    gimli-adm
gollum-adm      legolas-adm    samwise-adm

The command completed successfully.
```

รูปภาพที่ 6 Net Group “Domain Admins” /domain

ถ้าสนใจให้เข้าไปนำเสนอหรือต้องการข้อมูลเพิ่มเติมติดต่อได้ที่

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