EXTRAHOP

Detect and Defeat AD Attacks With ExtraHop Decryption

Uplevel your defense against AD attacks with ExtraHop's decryption and analysis

SOLUTION BRIEF

Active Directory (AD) is a high-value target for attackers, offering a direct path to high-privilege access and lateral movement. Attackers exploit several common factors to remain undetected:

- **Encrypted Protocols:** Malicious activities are hidden within encrypted AD protocols (LDAP, MSRPC, CMB, WSMAN), making it difficult to differentiate from legitimate traffic
- **Tool Misuse:** Attackers use approved, legitimate admin tools (BloodHound, Ntdsutil), making their behavior blend in
- **Detection Challenge:** Effectively identifying attackers requires decrypting these protocols to inspect the commands executed, revealing the smoking gun

The Challenges

Microsoft Active Directory's central role in most environments makes it a prime target for attackers, and for good reason. Obtaining access to high-privilege accounts grants malicious actors—from cyber criminals to nation-states—unfettered access to achieve their objectives within a victim's network. AD is usually the shortest path to escalating privileges and moving laterally. With this privileged access, malicious actors can sidestep many other security controls to evade detection and access critical business data with ease. This privileged access can often be extended to cloud-based systems and services via Microsoft's cloud-based identity and access solution, Microsoft Entra ID. This means that the attacker's access can spread from on-prem to the cloud or vice versa.

Malicious actors frequently leverage the encryption options of AD protocols (LDAP, MSRPC, SMB, and WSMAN) to hide their activities. When these protocols are encrypted, it is very difficult to distinguish normal behavior from malicious actions, allowing attackers to blend into the background. Traditional man-in-the-middle decryption solutions like NGFWs don't support decrypting many of these protocols and aren't situated to cover this kind of back-end, east-west traffic. To complicate matters, many of the same legitimate tools used by AD admins to manage and troubleshoot their AD environment are also used by attackers to enumerate the environment. So, simply setting detections around tools like BloodHound, SharpHound, PingCastle, and Ntdsutil won't be enough to positively identify malicious behavior. To confidently identify the malicious activity from the normal activity, you need a way to decrypt the protocols used and look inside those protocols at the actual commands being executed in order to find the smoking gun hidden within.

KEY CAPABILITIES

Eliminate the blind spots of your encrypted AD protocols by leveraging ExtraHop's unique out-of-band decryption solution

ExtraHop's strategic, out-of-band decryption introduces zero latency, operates at 100 Gb/sec throughput, and can't impact production traffic flow—giving you visibility without compromising resiliency

ExtraHop's cloud-scale machine learning applies scalable compute to multiple models to quickly and accurately surface anomaly-based and behavioral detections

Uplevel your Active Directory defense for the most prevalent types of AD attacks

How ExtraHop Solves the Challenges

ExtraHop decrypts and decodes TLS as well as SMB, WSMAN, RPC, NTLM, and Kerberos traffic to reveal attacks that have been hiding in encrypted channels.

- Decrypt not just TLS traffic but also NTLM, Kerberos, and other encrypted protocols used by AD
- After you decrypt, decode the protocols so you can see exactly what commands are executed
- Purpose-built detections look into decrypted and decoded conversations to spot known TPPs

In order to defend against encrypted AD attacks, solving just one problem isn't enough. You need to solve three separate problems:

First, we need a way to decrypt the AD protocols. Second, we need to decode and analyze those protocols to identify normal vs. malicious behavior. Third, we need detections to identify AD attacks in real time, at scale, before the attacker can move laterally and escalate privileges.

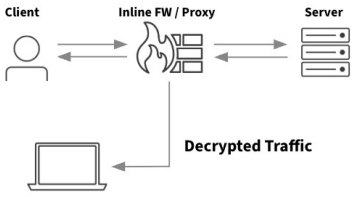
ExtraHop is the solution for all three problems. Unlike most solutions like next-gen firewalls, ExtraHop doesn't utilize man-in-the-middle decryption. This kind of in-line decryption has a few drawbacks, like introducing latency, potentially disrupting traffic flow, and more. Most importantly, it would be ineffectual for AD protocols like LDAP, RPC, SMBv3, and WSMAN that can utilize Kerberos or NTLM for encryption. And without decryption, you are blind.

ExtraHop is out-of-band rather than in-line, like a firewall. This means it's impossible for ExtraHop to introduce latency or cause real packets to be dropped. ExtraHop conducts all decryption and analytics "on box." This means it never needs to send any cleartext data across the network nor re-encrypt any messages.

ExtraHop accesses the ephemeral session secrets for each conversation with a lightweight secret-sharing agent installed on the Domain Controllers. The agent securely transmits session secrets across a PFS-encrypted channel to the ExtraHop sensor. ExtraHop then analyzes the decrypted protocols to provide rich analysis in real time, including machine-learning behavioral detections. ExtraHop decrypts TLS traffic in the same manner. This means ExtraHop has unparalleled visibility into ALL Kerberos, NTLM, and TLS encrypted protocols.

LEGACY APPROACH

MITM Decryption

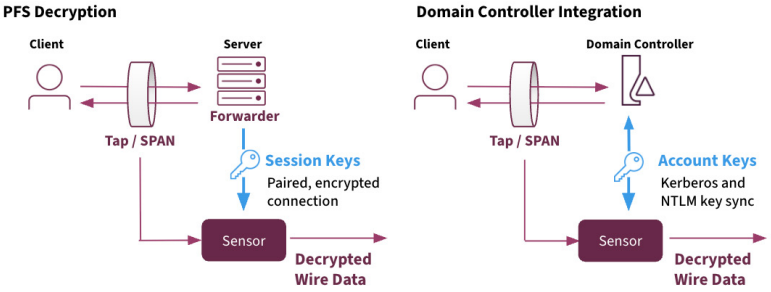


Disadvantages

- Typically blind to E/W traffic
- Introduces latency, doesn't scale
- High operational complexity

MODERN APPROACH

Strategic, Out-of-Band Decryption



ExtraHop Advantages

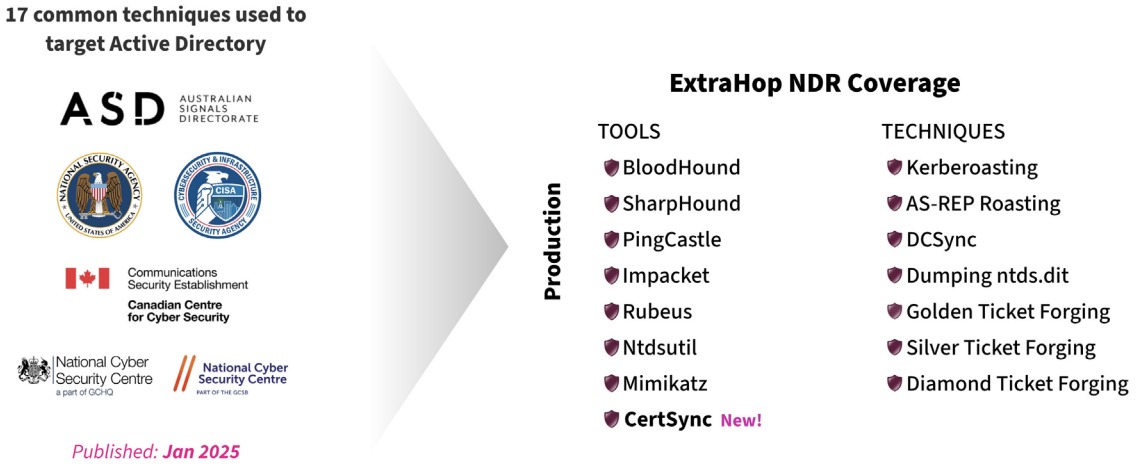
- N/S & E/W visibility
- Zero latency, scales to line speed
- Passive & invisible to attackers
- Maintain end-to-end encryption
- Low operational complexity

But visibility is just the first part of the problem. You still have hundreds of thousands of LDAP, WSMAN, and SMB transactions to watch every second. No one has a SOC large enough to inspect this volume of decrypted traffic for signs of attacks, but ExtraHop can. First, ExtraHop extracts all relevant data from both headers and payload and converts it to lightweight, compressible records. Records from all sensors are securely uploaded to your ExtraHop-managed cloud recordstore, where multiple machine-learning models analyze that data for anomalies that indicate an attack. This separation of duties between the CPU of the sensor and the elastic compute of the cloud models is what allows ExtraHop to scale up to 100 Gb/sec—the most scalable NDR solution on the market.

Finally, ExtraHop leverages a combination of anomaly, behavioral, statistical, and rules-based logic to trigger high-fidelity detections around the most pervasive AD tools and techniques like Impacket, Mimikatz, and BloodHound, as well as advanced techniques like Kerberoasting, remote command execution, SMB named pipe abuse, golden and silver ticket forging, DCSync attacks, and many more.

ExtraHop Coverage of the Top Active Directory Tools and Techniques

Top tools and techniques leveraged by threat actors reported by Five Eyes (FVEY) agencies & CISA



Because ExtraHop decrypts the traffic and sees the actual calls made over the network, you can drill down into the actual commands executed over the wire between hosts. This kind of granularity gives your team the ability to easily go from high-fidelity detection directly to the smoking gun, all in a single UI.

TAKE THE NEXT STEP

Learn more about how ExtraHop can help detect attacks despite encryption:
www.extrahop.com/resources/security/secure-decryption

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP®

info@extrahop.com
extrahop.com