Microsoft Active Directory as a Prime Target for Ransomware Operators

August 24, 2022
by Joseph Salazar & Juan Carlos Vázquez

The Active Directory (AD) infrastructure continues to be a key element in ransomware campaigns and post-compromise extortion, representing a significant threat to businesses. With the time between initial breach and impact being so short in a ransomware attack, the main area of concern for businesses is the challenge of quick detection.

Targeted businesses usually become aware of ransomware only after an adversary encrypts its assets to interrupt their availability. At this point, it is too late to do anything about the attack and they must shift immediately to executing their post-breach response plan.

Active Directory in the Crosshairs

By definition, Active Directory (AD) stores information about objects on a network in a logical, hierarchical manner making information easy for administrators and users to find and use. It uses a structured data store, known as the directory, as the basis for organizing the directory information (objects). These objects will typically include shared resources such as servers, volumes, printers, and user and computer accounts.

Cyber adversaries have increasingly set their sights on abusing Microsoft's AD since it serves as a neat gateway into the entirety of a network. Compromising AD allows adversaries to move laterally through the rest of the network, escalate privileges, obtain administrative access rights, and ultimately, encrypt and exfiltrate sensitive data.

Many legacy security solutions have proven ineffective against ransomware operators, who have developed tactics to evade or bypass traditional security controls. Although EDR solutions can protect endpoints, without Identity protection, a threat actor may compromise AD and increase their chances of finding holes in the network that can be exploited and used to launch ransomware attacks.

Businesses can greatly reduce the impact of such compromises as long as they can detect the threat early enough in the attack cycle. Early detection in the post-infiltration phase is where the SentinelOne® Identity solution excels.

Ransomware Case Studies

Let's examine three recent case studies by The DFIR Report in which ransomware gangs targeted Microsoft AD as part of their tactics.

1. **Bumblebee Ransomware**
   This case study details an attempted ransomware deployment using a malware loader called BumbleBee. Initial execution began with a password protected zipped ISO file that likely originated from a malicious email. After a user opened the file containing BumbleBee, it dropped a Cobalt Strike beacon and proceeded to inject into various other processes on the host.The adversary in this attack was noted to have started AD discovery using ADFind only four hours after initial breach and, later in the attack timeline, searched for control to a more privileged account. Investigations showed that the adversary enumerated AD on three different occasions over an 11-day dwell period through ADFind.
2. **Quantum Ransomware**
   In "one of the fastest ransomware cases" observed by The DFIR Report, cyber adversaries gained initial access and deployed domain-wide ransomware in under four hours through an IcedID payload delivered via email.After a user clicked the malicious files, a collection of discovery tasks were executed within Windows built-in utilities and established persistence in the host. Two hours later, the adversaries deployed Cobalt Strike followed by the use of ADFind to perform discovery of the target organizations' AD structure.During this intrusion, it was discovered that the adversaries managed to steal administrator account credentials which enabled them to spread laterally across the AD domain.
3. **Conti Ransomware**
   Cyber adversaries don't take holidays. In fact, public holidays, long weekends, and off hours are when they thrive. In this case study, the adversaries remained dormant over a 19-day dwell time before deploying Conti ransomware shortly after Christmas, resulting in domain-wide encryption.The investigation found that the adversaries utilized IcedID as an initial access vector to drop a Cobalt Strike beacon on a compromised host and then established persistence in the environment by installing remote management tools Atera and Splashtop. Notably, there were many attempts to exploit CVE-2021-42278 and CVE-2021-42287; both known AD vulnerabilities often used to create privileged accounts.

Reducing adversary dwell times is vital in an age where attackers have a plethora of tools at their disposal to gain privileged access to internal corporate networks. Widespread IT and AD hygiene issues coupled with weak detection capabilities that do not detect the techniques used in ransomware attacks leave many enterprises exposed to devastating compromises.

Preventing Ransomware Encryption Isn't Enough

Ransomware operators attacking enterprises have evolved their tactics beyond simple encryption, using double or even triple extortion techniques, exposing their victim's data to increase the level of coercion.

Organizations that refuse to pay ransom demands are exposed to economic and reputational harm as attackers threaten to make stolen data available on ransomware leak sites or to sell it on the darknet to other threat actors. The technique, pioneered by the Maze ransomware gang, has been widely copied and extended by other operators.

Threats to leak data if victims approach law enforcement, negotiation or incident response firms pile on the pressure to pay up and pay early – most ransomware operators will increase their demands the longer victims hold out.

In human-operated ransomware attacks, the threat actors typically perform internal reconnaissance and move laterally through the compromised networks to profile their victims, targeting the organization's most critical assets so they can negotiate from a stronger position. The use of "Living off the Land" techniques and tools coupled with leveraging AD to deploy the ransomware via Group Policy Objects (GPOs) is prevalent in recent attacks.

Essential Questions in Ransomware Preparedness Assessment

A ransomware preparedness assessment can help ensure the organization has a strong security posture to prevent and contain ransomware attacks. Some key questions the organization should seek to answer include:

- How can the organization identify malicious actors on the AD infrastructure and differentiate them from organizational assets? Does the security team have the tools to separate legitimate queries to AD from malicious ones?
- How does the business prevent the use of tools like Bloodhound or Mimikatz? Should the EPP/EDR solution contain or alert when malicious tools like these are used?
- How can the security team identify when exposed credentials on other endpoints are vulnerable to exploit?
- How can the organization restrict connectivity and trust relationships within AD across different areas of the company to prevent the spread of ransomware attacks?
- What tools are available to identify when attackers are exploiting privileged accounts, such as AD domain admins, service accounts, or shadow admins possessing privileges at the endpoints?
- Is the business currently able to protect data from tampering by unauthorized programs or ransomware?
- How can the security team isolate the attack source when investigation confirms the presence of domain controller enumeration or "credential dumping" events?

The SentinelOne Singularity™ Identity Solution

The SentinelOne Singularity™ Identity solution works with existing security controls to address the ransomware problem. Good EDR solutions detect most ransomware variants in use today. However, should attackers find a way through the organization's first line of defense, Singularity™ Identity provides detection capabilities for discovery, lateral movement, privilege escalation, and data gathering activities used in ransomware attacks.

Singularity™ Identity offers coverage across different layers including the network, endpoint, data, applications, and AD, providing early and accurate detection while preventing attackers from accessing sensitive or critical data, credentials, and other objects.

The Singularity™ Identity solution prevents attackers from breaking out of a compromised system by restricting their ability to conduct reconnaissance or move laterally to production assets. Further, it denies cyber adversaries the ability to discover or list domain controllers, domain memberships, group privileges, and other AD objects while providing early and accurate alerts on the activity. It returns data that leads the adversaries to decoys for engagement, identifying their tactics, technique, and procedures and providing telemetry on the tools they used to extract the data from AD.

Simply put, the solution immediately misdirects and misinforms the adversaries as soon as they look or attempt to move around, diverting them to the decoy environment and reducing the impact on production infrastructure. Singularity Identity also provides detailed event data, displays visual attack replays, and collects forensic evidence for analysis and threat intelligence development to raise the security posture and defend against subsequent attacks.

Finally, Singularity™ Identity's concealment capability hides and denies access to local files, folders, removable devices, and mapped network or cloud shares, preventing adversaries from enumerating, accessing, encrypting, or even exfiltrating them from the organization. Simultaneously, the solution maps fake file shares that lead to decoy servers for the ransomware to discover and encrypt. As the malware attempts to encrypt the data it finds, the Identity solution rate-limits the connection and feeds the ransomware with endless streams of data to encrypt. This delay stalls the attack, giving the security teams time to isolate infected systems and stop further damage quickly.

Conclusion

Protecting against modern ransomware attacks takes preparation and overlapping security controls that provide a layered defense that sophisticated attackers must penetrate undetected. Deploying the SentinelOne Singularity™ Identity solution as a layer in that defensive strategy enhances existing security controls while providing unique denial, detection, and derailment functions to elevate the security posture and harden the organization against ransomware attacks.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- How Kerberos Golden Ticket Attacks Are Signaling a Greater Need for Identity-Based Security
- Detecting Unconstrained Delegation Exposures in AD Environment
- Detecting a Rogue Domain Controller – DCShadow Attack
- Endpoint, Identity and Cloud | Top Cyber Attacks of 2022 (So Far)
- Dollar Signs in Attackers' Eyes | How to Mitigate CVE-2022-26923
- Top 10 Ways to Protect Your Active Directory