How to Protect Active Directory Against Ransomware Attacks

tenable.com/blog/how-to-protect-active-directory-against-ransomware-attacks

June 14, 2021

Tenable Blog

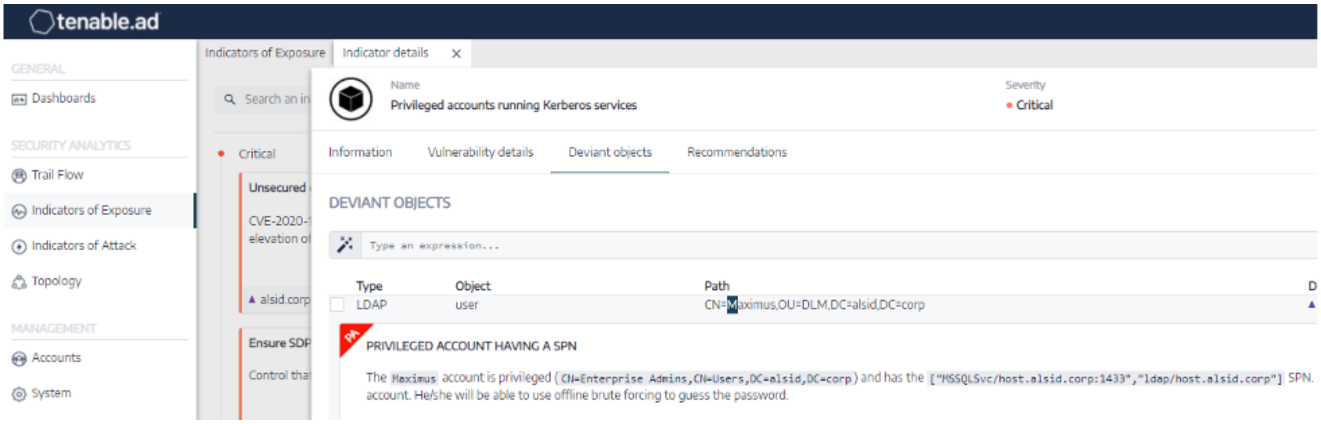
Subscribe

Ransomware attacks every type of organization from every angle and Active Directory remains the common target. Stop privilege escalation by fixing these key AD and group policy misconfigurations.

Ransomware has struck every type of organization around the world. It's changed dramatically, too, entering the enterprise from nearly every angle, with attackers leveraging stolen data by posting it on the internet to force victims to pay. In most cases (see SolarWinds and XingLocker), Active Directory (AD) is targeted so the attacker can easily distribute the ransomware after obtaining domain privileges. There are, however, ways to help secure Active Directory to prevent ransomware from succeeding.

Distinct areas within Active Directory can be secured, which will increase the overall security of the enterprise and reduce the security risk at the same time. Specifically, the following settings around AD objects can be secured. Here's how:

- Misconfigurations of user attributes need to be fixed
- Misconfigurations of groups need to be fixed
- Privileged groups need to be cleaned up
- AD processes need to have correct configurations (e.g. SDProp)
- Service principal names (SPNs) need to be secured (shown in Figure 1)
- Trust relationships need to be correct and secured
- SidHistory attribute needs to be cleaned up for users



Name
Privileged accounts running Kerberos services

Severity
Critical

DEVIANT OBJECTS

Type	Object	Path	D
LDAP	user	CN=Maximus,OU=DLM,DC=alsid,DC=corp	▲

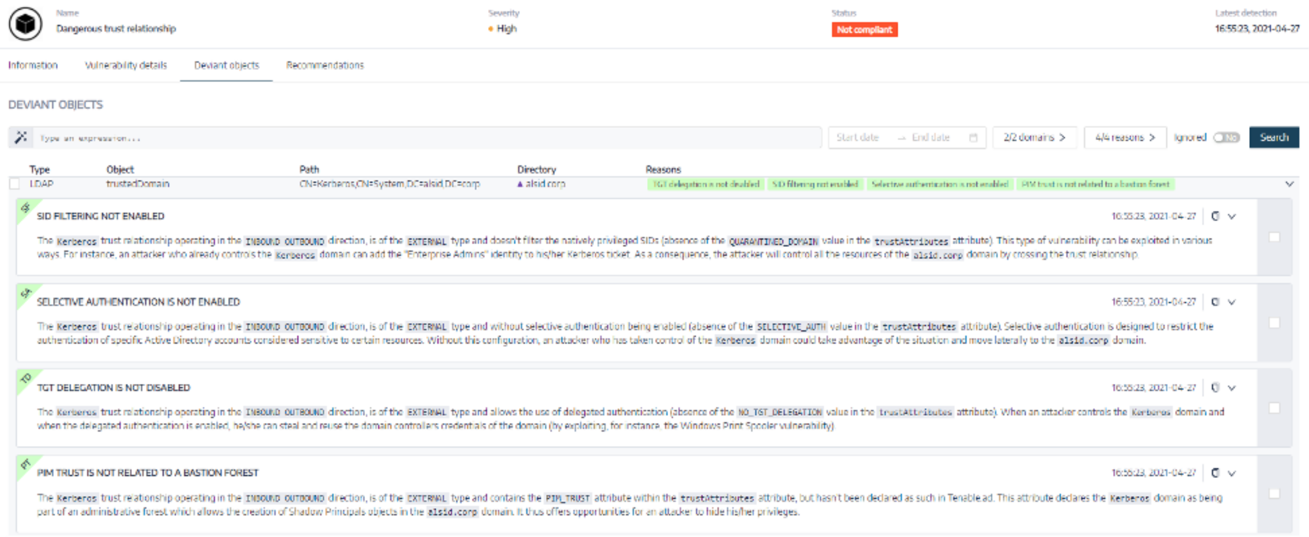
PRIVILEGED ACCOUNT HAVING A SPN

The `Maximus` account is privileged (`CN=Enterprise Admins,CN=Users,DC=alsid,DC=corp`) and has the `["MSSQLSvc/host.alsid.corp:1433","ldap/host.alsid.corp"]` SPN. account. He/she will be able to use offline brute forcing to guess the password.

Figure 1. User account with Service Principal Name (SPN)

In addition, AD itself and group policy can be secured to ensure the attacker can't leverage misconfigurations and areas where privilege escalation can be achieved. Here's how:

- AD trusts need to be verified and secured (shown in Figure 2)
- AD delegations need to be cleaned up
- Group policy delegations need to be cleaned up
- Group policy structural components need to be secured
- Security settings deployed by group policy objects need to be enabled



Name: Dangerous trust relationship
Severity: High
Status: Not compliant
Latest detection: 16:55:23, 2021-04-27

DEVIANT OBJECTS

Type	Object	Path	Directory	Reasons
LDAP	trustedDomain	CN=Kerberos,CN=System,DC=alsid,DC=corp	alsid.corp	TGT delegation is not disabled SID filtering not enabled Selective authentication is not enabled PIM trust is not related to a bastion forest

SID FILTERING NOT ENABLED — 16:55:23, 2021-04-27

The `Kerberos` trust relationship operating in the `INBOUND OUTBOUND` direction, is of the `EXTERNAL` type and doesn't filter the natively privileged SIDs (absence of the `QUARANTINED_DOMAIN` value in the `trustAttributes` attribute). This type of vulnerability can be exploited in various ways. For instance, an attacker who already controls the `Kerberos` domain can add the "Enterprise Admins" identity to his/her Kerberos ticket. As a consequence, the attacker will control all the resources of the `alsid.corp` domain by crossing the trust relationship.

SELECTIVE AUTHENTICATION IS NOT ENABLED — 16:55:23, 2021-04-27

The `Kerberos` trust relationship operating in the `INBOUND OUTBOUND` direction, is of the `EXTERNAL` type and without selective authentication being enabled (absence of the `SELECTIVE_AUTH` value in the `trustAttributes` attribute). Selective authentication is designed to restrict the authentication of specific Active Directory accounts considered sensitive to certain resources. Without this configuration, an attacker who has taken control of the `Kerberos` domain could take advantage of the situation and move laterally to the `alsid.corp` domain.

TGT DELEGATION IS NOT DISABLED — 16:55:23, 2021-04-27

The `Kerberos` trust relationship operating in the `INBOUND OUTBOUND` direction, is of the `EXTERNAL` type and allows the use of delegated authentication (absence of the `NO_TGT_DELEGATION` value in the `trustAttributes` attribute). When an attacker controls the `Kerberos` domain and when the delegated authentication is enabled, he/she can steal and reuse the domain controllers credentials of the domain (by exploiting, for instance, the Windows Print Spooler vulnerability).

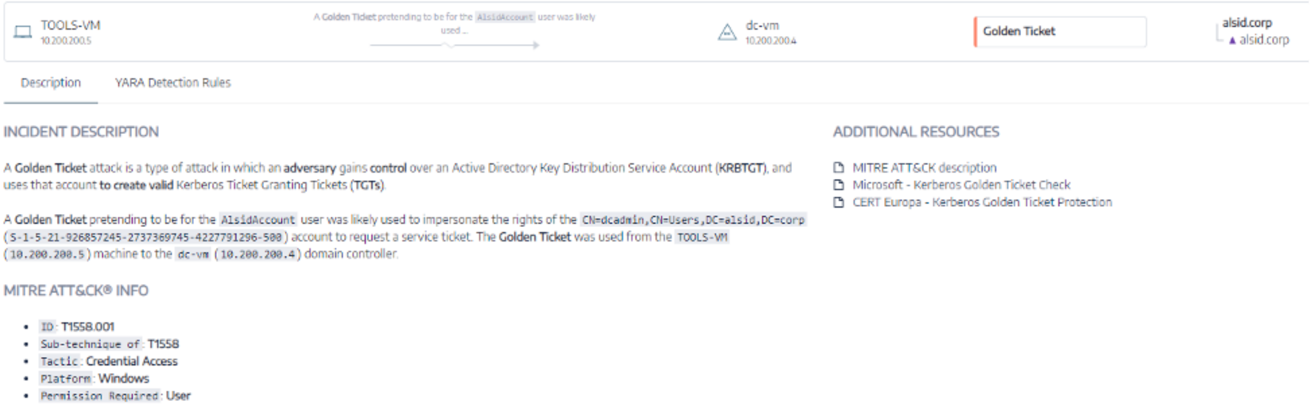
PIM TRUST IS NOT RELATED TO A BASTION FOREST — 16:55:23, 2021-04-27

The `Kerberos` trust relationship operating in the `INBOUND OUTBOUND` direction, is of the `EXTERNAL` type and contains the `PIM_TRUST` attribute within the `trustAttributes` attribute, but hasn't been declared as such in Tenable.ad. This attribute declares the `Kerberos` domain as being part of an administrative forest which allows the creation of Shadow Principals objects in the `alsid.corp` domain. It thus offers opportunities for an attacker to hide his/her privileges.

Figure 2. Mergers and acquisitions can orphan trusts; in addition, required trusts need to be secured.

Finally, attackers want to gain privileges. Once privileges are obtained, they want to create backdoors. Being able to detect these types of AD attacks is essential. Below are some of the actions AD admins and security pros can take to disrupt attack paths:

- Ensure privileged group membership is monitored
- Detect DCShadow and DCSync attacks
- Golden Ticket attacks (illustrated in Figure 3)
- Detect lateral movement attacks
- Detect dangerous SIDHistory and PrimaryGroupID settings



INCIDENT DESCRIPTION

A **Golden Ticket** attack is a type of attack in which an **adversary** gains **control** over an Active Directory Key Distribution Service Account (**KRBTGT**), and uses that account **to create valid** Kerberos Ticket Granting Tickets (**TGTs**).

A **Golden Ticket** pretending to be for the `AlsidAccount` user was likely used to impersonate the rights of the `CN=dcadmin,CN=Users,DC=alsid,DC=corp` (`S-1-5-21-926857245-2737369745-4227791296-500`) account to request a service ticket. The **Golden Ticket** was used from the `TOOLS-VM` (`10.200.200.5`) machine to the `dc-vm` (`10.200.200.4`) domain controller.

MITRE ATT&CK® INFO

- `ID`: T1558.001
- `Sub-technique of`: T1558
- `Tactic`: Credential Access
- `Platform`: Windows
- `Permission Required`: User

ADDITIONAL RESOURCES

- MITRE ATT&CK description
- Microsoft - Kerberos Golden Ticket Check
- CERT Europa - Kerberos Golden Ticket Protection

Figure 3. Tenable.ad can detect advanced attacks on Active Directory, in real time, with no agent or privilege.

Technology is available to continuously and automatically analyze and detect AD security and attack paths. To find out more about how Tenable.ad can help, view this webinar: Introducing Tenable.ad — Secure Active Directory and Disrupt Attack Paths

Learn More

- View the webinar: Introducing Tenable.ad — Secure Active Directory and Disrupt Attack Paths
- Download the E-book: A King's Ransom: How to Stop Ransomware Spreading via AD
- Read the Active Directory blog posts

Derek Melber

Derek Melber is a leading technical instructor, author and consultant who comes to Tenable by way of the Alsid acquisition. He is a 16-time Microsoft MVP with deep knowledge of Group Policy, Active Directory, desktop management and Windows security. As a public speaker and technology evangelist, he has educated AD administrators in over 30 countries about how to efficiently and effectively secure Active Directory and Azure AD. He has published a broad range of educational content, including books, articles and videos, that demystify the most complex and technical subjects in an energetic and understandable style.

Related Articles

How State and Local Governments Can Bolster their Cyber Defenses

May 24, 2022
Cyber security leaders of U.S. cities and states must protect their systems and data from nation-state attackers, including Russian hackers. President Biden has warned of potential Russian cyberatt...

By Matt Kucik

How To Make Your SOC Identity-Aware and Efficient

May 23, 2022
While an attacker only needs to be right once, security teams must be right every time. That's why it's critical for SOC teams to stop ransomware attackers from exploiting AD weaknesses.

Anjali George

Tenable’s Acquisition Of Cymptom: An “Attack Path-Informed” Approach to Cybersecurity

February 17, 2022
Tenable’s recent acquisitions all had the same overarching goal: helping our customers gain better security insights across their cyberattack surface.

Nico Popp

- Active Directory
- Government
- Threat Management

Thank You

Thank you for your interest in Tenable.io. A representative will be in touch soon.

Try for Free Buy Now

Try Nessus Professional Free

FREE FOR 7 DAYS
Nessus® is the most comprehensive vulnerability scanner on the market today. Nessus Professional will help automate the vulnerability scanning process, save time in your compliance cycles and allow you to engage your IT team.

Buy Nessus Professional

Nessus® is the most comprehensive vulnerability scanner on the market today. Nessus Professional will help automate the vulnerability scanning process, save time in your compliance cycles and allow you to engage your IT team.

Buy a multi-year license and save. Add Advanced Support for access to phone, community and chat support 24 hours a day, 365 days a year.

Select Your License

Buy a multi-year license and save.

Add Support and Training

Buy Now
Renew an existing license | Find a reseller
*VAT incl.

Try for Free Buy Now
Tenable.io FREE FOR 30 DAYS
Enjoy full access to a modern, cloud-based vulnerability management platform that enables you to see and track all of your assets with unmatched accuracy.

Tenable.io BUY
Enjoy full access to a modern, cloud-based vulnerability management platform that enables you to see and track all of your assets with unmatched accuracy. **Purchase your annual subscription today.**

65 assets

Choose Your Subscription Option:

Buy Now
Please contact us or a Tenable partner.

Thank You

Thank you for your interest in Tenable.io. A representative will be in touch soon.

Try for Free Buy Now

Try Tenable.io Web Application Scanning

FREE FOR 30 DAYS
Enjoy full access to our latest web application scanning offering designed for modern applications as part of the Tenable.io platform. Safely scan your entire online portfolio for vulnerabilities with a high degree of accuracy without heavy manual effort or disruption to critical web applications. **Sign up now.**

Buy Tenable.io Web Application Scanning

Enjoy full access to a modern, cloud-based vulnerability management platform that enables you to see and track all of your assets with unmatched accuracy. **Purchase your annual subscription today.**

5 FQDNs

$3,578

Buy Now

Please contact us or a Tenable partner.

Thank You

Thank you for your interest in Tenable.io Web Application Scanning. A representative will be in touch soon.

Try for Free Contact Sales

Try Tenable.io Container Security

FREE FOR 30 DAYS

Enjoy full access to the only container security offering integrated into a vulnerability management platform. Monitor container images for vulnerabilities, malware and policy violations. Integrate with continuous integration and continuous deployment (CI/CD) systems to support DevOps practices, strengthen security and support enterprise policy compliance.

Buy Tenable.io Container Security

Tenable.io Container Security seamlessly and securely enables DevOps processes by providing visibility into the security of container images – including vulnerabilities, malware and policy violations – through integration with the build process.

Thank You

Thank you for your interest in the Tenable.io Container Security program. A representative will be in touch soon.

Try for Free Contact Sales

Try Tenable Lumin

FREE FOR 30 DAYS
Visualize and explore your Cyber Exposure, track risk reduction over time and benchmark against your peers with Tenable Lumin.

Buy Tenable Lumin

Contact a Sales Representative to see how Lumin can help you gain insight across your entire organization and manage cyber risk.

Thank You

Thank you for your interest in Tenable Lumin. A representative will be in touch soon.

Request a demo of Tenable.sc

Please fill out this form with your contact information.

A sales representative will contact you shortly to schedule a demo.
** Field is required*

Request a demo of Tenable.ot

Get the Operational Technology Security You Need.

Reduce the Risk You Don’t.