On April 24, 2022, a privilege escalation hacking tool, KrbRelayUp, was publicly disclosed on GitHub by security researcher Mor Davidovich. KrbRelayUp is a wrapper that can streamline the use of some features in Rubeus, KrbRelay, SCMUACBypass, PowerMad/SharpMad, Whisker, and ADCSPwn tools in attacks.

Although this attack won't function for Azure Active Directory (Azure AD) joined devices, hybrid joined devices with on-premises domain controllers remain vulnerable. Microsoft Defender for Identity detects activity from the early stages of the attack chain by monitoring anomalous behavior as seen by the domain controller. In addition, signals from Defender for Identity also feed into Microsoft 365 Defender, providing organizations with a comprehensive solution that detects and blocks suspicious network activities, malicious files, and other related components of this attack. Microsoft Defender Antivirus detects this attack tool as the malware family HackTool:MSIL/KrbUpRly.

Microsoft encourages customers to update Domain Controller: LDAP server signing requirements to Require signing as detailed in this advisory and enable Extended Protection for Authentication (EPA) as detailed in this blog.

Originally, KrbRelayUp supported only one method that's based on taking advantage of resource-based constrained delegation (RBCD); it later added several additional attack methods. In this blog, we discuss RBCD to provide further insights into how the initial KrbRelayUp attack method works. We also detail the stages that make up the said attack. Finally, we provide recommendations and guidelines that can help organizations strengthen their device configurations and defend their networks from attacks that use this tool.

Understanding the attack: What is resource-based constrained delegation?

Resource-based constrained delegation (RBCD) represents the key to this attack method, enabling the tool to impersonate an administrator and eventually run a code as the SYSTEM account of a compromised device.

Authentication protocol basics

An authentication protocol verifies the legitimacy of a resource or identity. When a user signs into a website, that website uses a methodology to confirm the authenticity of the resource requesting access. In simpler terms, the authentication process involves signing in with a password——made possible by the user knowing the password anticipated by the website. The Kerberos protocol serves as the main authentication framework for this process in on-premises Active Directory.

Delegation

Sometimes, however, a resource needs to request access to another resource on behalf of a different identity. A common example of this is mail delegation, wherein executives often give delegation rights to their executive assistants to send and receive emails on their behalf without providing the assistant with the executive's password. The executive assistant isn't authenticating as the executive; the executive has just allowed the assistant's account to "pretend" that they are.

Resource-based constrained delegation

Initially, only users with the SeEnableDelegation role could configure delegation, typically domain admins. These domain admins can manage resources and dictate which identities can act on behalf of a different resource. They achieve this by updating the msDS-AllowedToDelegateTo property of a user account or device. This property contains a list of all the unique identifiers (service principal names, or SPNs) to which this object can delegate or act on behalf of.

However, as organizations expanded, administrators struggled to manage all the delegation requirements, raising the need for a new type of delegation: resource-based. For instance, in an organization with several file servers that all trust a web server for delegation, an admin would have to change the msDS-AllowedToDelegateTo priority in all of the different file servers to introduce a second web server. With resource-based delegation, the list of trusted computers is held on the receiving end. Thus, in our example, only the newly created server would require a change of settings.

Unsigned LDAP and relay attacks

For the RBCD method of the KrbRelayUp tool to work, the LDAP protocol must not use signing to communicate between LDAP clients and domain controllers. While this setting is still the default on Windows, as of 2019 Microsoft recommends configuring LDAP to use LDAP channel binding and signing.

LDAP is one of the main protocols that directory services tools, such as Active Directory, use to query and access directory information. By default, LDAP is vulnerable to credential relaying attacks. For example, in a credential relaying attack, a web server requesting a password to sign in would have its request relayed by an attacker to an authorized client. The attacker then relays the client reply containing the correct password back to the server, thus signing in. Once the attacker is signed in, they have the same permissions as the user whose credentials were relayed.

If LDAP signing is required, each request to the server needs to be cryptographically signed. In this case, the attacker would still be able to relay the sign-in request and reply, but all further requests from the attacker would be disregarded because each request must be signed, and the attacker doesn't have the proper keys to do the signing.

Ms-DS-MachineAccountQuota

The final key concept behind the RBCD method of KrbRelayUp tool is the ms-DS-MachineAccountQuota attribute, which all User Active Directory objects have. This attribute is set to 10 by default, which means that any user in Active Directory can create up to 10 computer accounts associated with them. The legitimate usage of this attribute is to allow users to have multiple devices on a network that belong to them that they can then manage. However, if a compromised user doesn't have 10 actual devices associated with their account, an attacker can create an account for a non-existing device that will be an object in Active Directory. This fake computer account isn't associated with a real device but can perform Active Directory authentication requests as if it were.

Initially, the ability to obtain such an account was a prerequisite for this attack method, but since the release of the tool, other security researchers found ways to get around this requirement.

KrbRelayUp attack flow

To launch an attack using the RBCD method of KrbRelayUp, an attacker performs four main steps:

Step 1: Acquisition of a suitable resource

The attacker first obtains a resource suitable to be the source of an RBCD. There are several ways to obtain such a resource; the most straightforward way is to create a new computer account as discussed above.

Step 2: Modification of the msDS-AllowedToActOnBehalfOfOtherIdentity attribute

Next, the attacker adds their resource to the current device's list of trusted resources. To do this, the attacker starts an LDAP session and relays the credentials of the current device to the LDAP server.

The new KrbRelayUp tool implements this step with these two smaller consecutive actions:

1. Authenticates to the LDAP service by triggering and performing a Kerberos relay attack
2. Edits the msDS-AllowedToActOnBehalfOfOtherIdentity attribute to add the attacker's resource to the list of entities permitted to delegate the target device.

Step 3: Privileged ticket acquisition

Here, the attacker leverages their control over their resource gained through the first step with the trust for their resource gained through the second step. As such, the local device trusts the attacker's resource to request a ticket addressed to the host SPN as the domain administrator. The request is made by first pretending to be the attacker's resource and consists of three requests:

1. AS-Req – A request to generate a Ticket Granting Ticket (TGT) for the attacker's impersonated resource.
2. S4U2self – A request to generate a Ticket Granting Service (TGS) ticket from an administrator to the resource.
3. S4U2proxy – A request to generate a TGS ticket for the host SPN as an administrator delegating their access via the impersonated resource.

After this step, the attacker has a valid ticket for the local device that allows the administrator to be impersonated.

Step 4: Privileged ticket leverage

The last step leverages the attacker's newly acquired ticket to run code on the device. In the attack, as it's published online, the Service Control Manager (SCM) is asked to create a new service with SYSTEM permissions.

Protecting against KrbRelayUp attacks through coordinated threat defense

It's important to note that KrbRelayUp cannot be used in attacks against organizations that are only using Azure AD. However, in hybrid identity environments where organizations synchronize their domain controllers with Azure AD, if an attacker compromises an Azure virtual machine using a synchronized account, they'll receive SYSTEM privileges on the virtual machine.

To reduce the impact of this threat, organizations should apply the mitigations below. Microsoft 365 Defender customers can check the recommendations card for the deployment status of monitored mitigations.

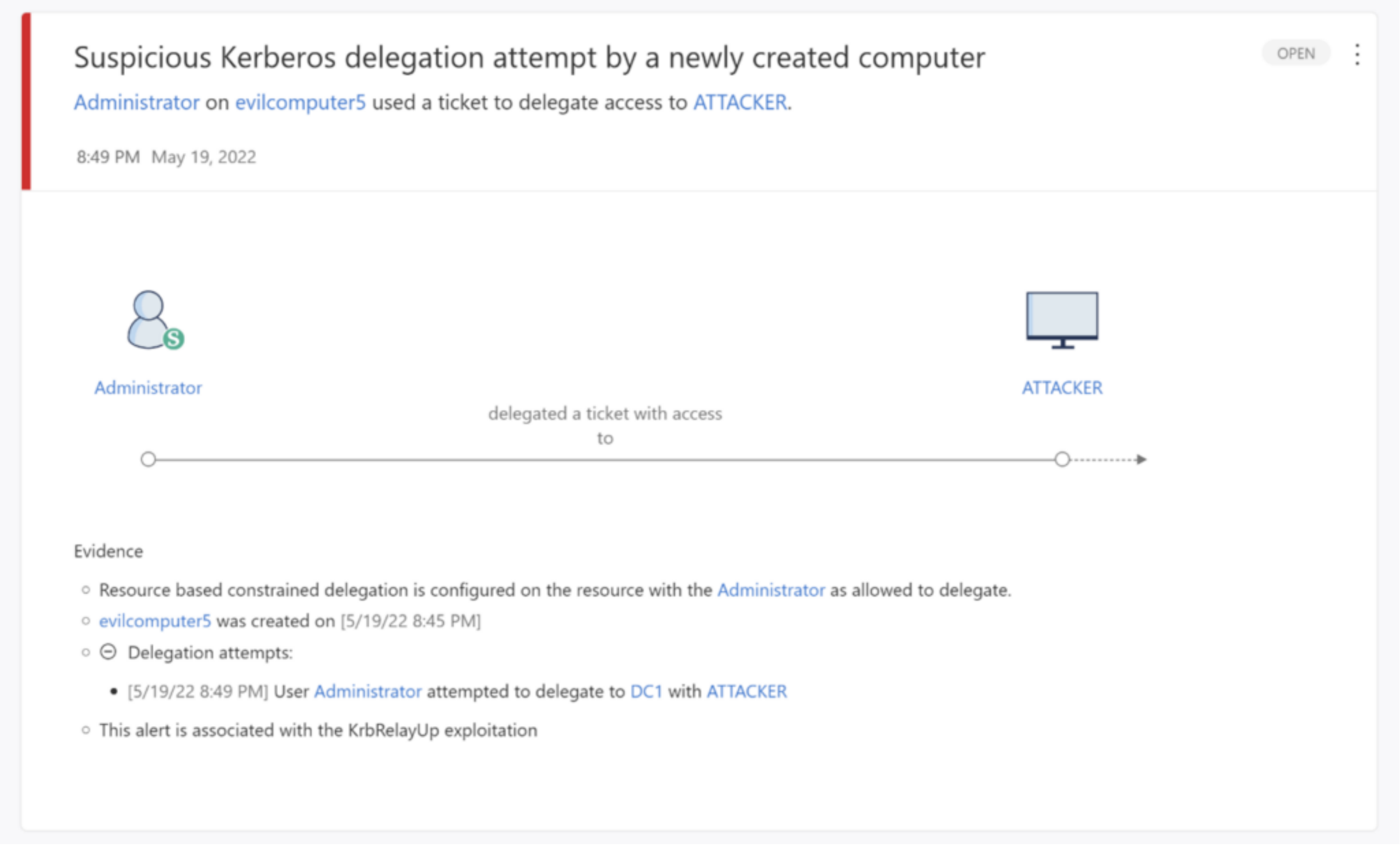
- Microsoft has provided guidance for enabling LDAP channel binding and LDAP signing. Microsoft recommends that administrators configure LDAP signing and LDAP channel binding as recommended in the said advisory and described in detail in 2020 LDAP channel binding and LDAP signing requirements for Windows (KB4520412).
- Organizations should also consider setting the ms-DS-MachineAccountQuota attribute to 0 to make it more difficult for an attacker to leverage the attribute for attacks. Setting the attribute to 0 stops non-admin users from adding new devices to the domain, blocking the most effective method to carry out the attack's first step and forcing attackers to choose more complex methods to acquire a suitable resource.

Detection details

Organizations should also deploy a comprehensive security solution like Microsoft 365 Defender to detect and block this threat across the stages of the attack chain. Microsoft 365 Defender has multiple layers of dynamic protection technologies, including machine learning-based protection, and correlates threat data from email, endpoints, identities, and cloud apps to provide in-depth and coordinated threat defense. All of these are backed by threat experts who continuously monitor the threat landscape for new attacker tools and techniques.

Microsoft Defender for Identity detects activity from the first three steps of the attack flow by monitoring anomalous behavior as seen by the domain controller. Starting in version 2.180, Defender for Identity has two detections that raise an alert when this attack is attempted:

- Suspicious Kerberos delegation attempt by a newly created computer.
- Suspicious edit of the Resource Based Constrained Delegation Attribute by a machine account (KrbRelayUp).


Suspicious Kerberos delegation attempt by a newly created computer

Administrator on evilcomputer5 used a ticket to delegate access to ATTACKER.

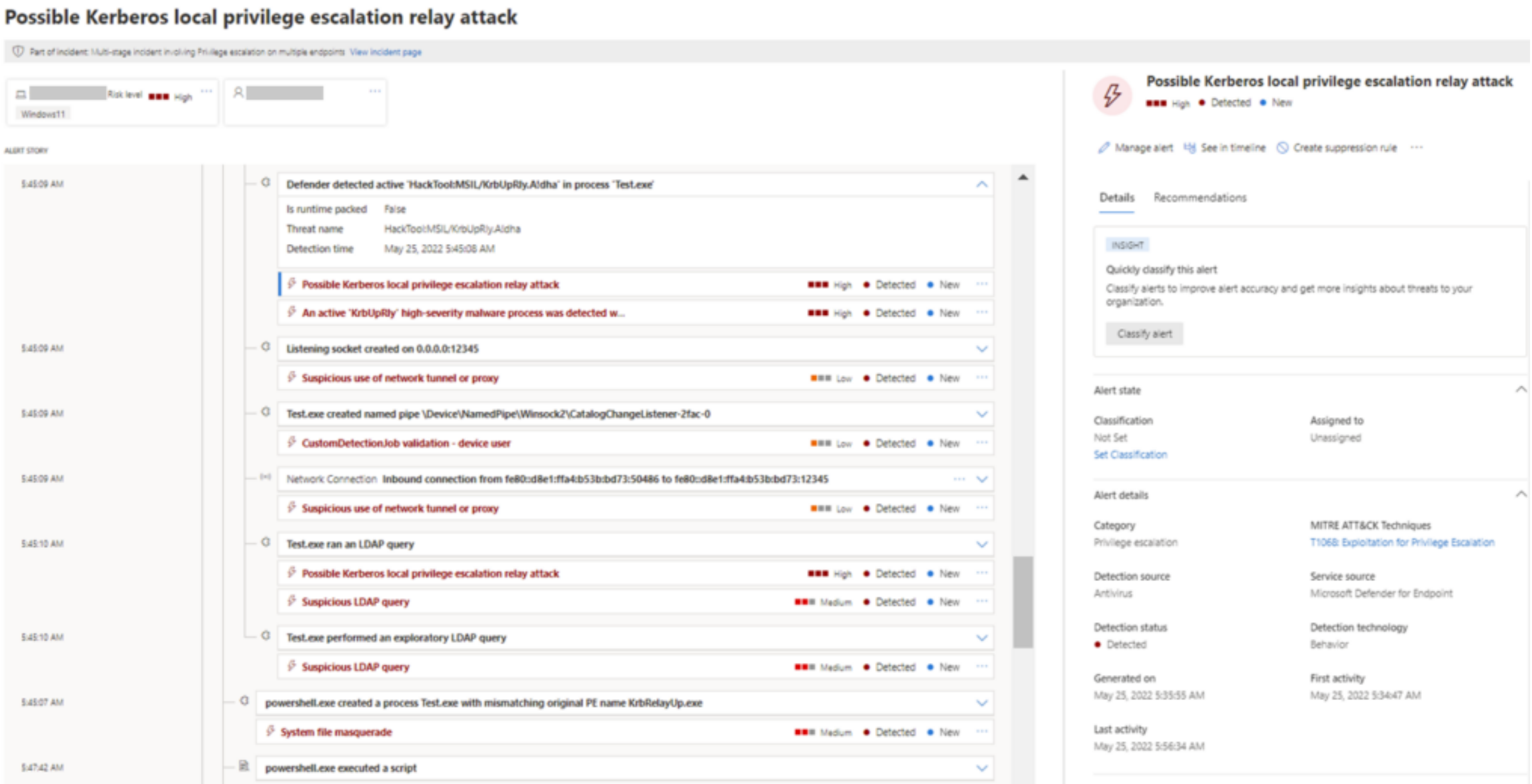
8:49 PM May 19, 2022

Evidence

- Resource based constrained delegation is configured on the resource with the Administrator as allowed to delegate.
- evilcomputer5 was created on [5/19/22 8:45 PM]
- ⊖ Delegation attempts:
  - [5/19/22 8:49 PM] User Administrator attempted to delegate to DC1 with ATTACKER
- This alert is associated with the KrbRelayUp exploitation

Figure 1. 'Suspicious Kerberos delegation attempt by a newly created computer' alert in Microsoft Defender for Identity

Microsoft Defender for Endpoint includes new and enhanced network inspection capabilities to correlate network and endpoint signals and emit high-confidence alerts. Defender for Endpoint leverages these network signals and looks for suspicious LDAP and Kerberos requests to Active Directory domain controllers to accurately detect attacks using KrbRelayUp. Defender for Endpoint also detects suspicious Kerberos sign-ins and service creations.



Possible Kerberos local privilege escalation relay attack

Part of incident: Multi-stage incident involving Privilege escalation on multiple endpoints View incident page

[redacted] Risk level ■■■ High

Windows11

[redacted]

ALERT STORY

5:45:09 AM Defender detected active 'HackTool:MSIL/KrbUpRly.A!dha' in process 'Test.exe'

Is runtime packed False
Threat name HackTool:MSIL/KrbUpRly.A!dha
Detection time May 25, 2022 5:45:08 AM

Possible Kerberos local privilege escalation relay attack ■■■ High ● Detected ● New

An active 'KrbUpRly' high-severity malware process was detected w... ■■■ High ● Detected ● New

5:45:09 AM Listening socket created on 0.0.0.0:12345

Suspicious use of network tunnel or proxy ■■■ Low ● Detected ● New

5:45:09 AM Test.exe created named pipe \Device\NamedPipe\Winsock2\CatalogChangeListener-2fac-0

CustomDetectionJob validation - device user ■■■ Low ● Detected ● New

5:45:09 AM Network Connection Inbound connection from fe80::d8e1:ffa4:b53b:bd73:50486 to fe80::d8e1:ffa4:b53b:bd73:12345

Suspicious use of network tunnel or proxy ■■■ Low ● Detected ● New

5:45:10 AM Test.exe ran an LDAP query

Possible Kerberos local privilege escalation relay attack ■■■ High ● Detected ● New

Suspicious LDAP query ■■■ Medium ● Detected ● New

5:45:10 AM Test.exe performed an exploratory LDAP query

Suspicious LDAP query ■■■ Medium ● Detected ● New

5:45:07 AM powershell.exe created a process Test.exe with mismatching original PE name KrbRelayUp.exe

System file masquerade ■■■ Medium ● Detected ● New

5:47:42 AM powershell.exe executed a script

Possible Kerberos local privilege escalation relay attack

■■■ High ● Detected ● New

Manage alert See in timeline Create suppression rule

Details Recommendations

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification: Not Set
Set Classification

Assigned to: Unassigned

Alert details

Category: Privilege escalation

MITRE ATT&CK Techniques: T1068: Exploitation for Privilege Escalation

Detection source: Antivirus

Service source: Microsoft Defender for Endpoint

Detection status: ● Detected

Detection technology: Behavior

Generated on: May 25, 2022 5:35:55 AM

First activity: May 25, 2022 5:34:47 AM

Last activity: May 25, 2022 5:56:34 AM

Figure 2. 'Possible Kerberos local privilege escalation relay attack' alert in Microsoft Defender for Endpoint

Microsoft Defender Antivirus detects a threat from the KrbRelayUp tool as the following malware:

- HackTool:MSIL/KrbUpRly.A
- HackTool:MSIL/KrbUpRly.C
- HackTool:MSIL/KrbUpRly.D

Microsoft 365 Defender customers may refer to the threat analytics report to determine if this threat is present in their network and to get additional details and recommendations. Threat analytics enables organizations to assess the impact of a threat to their network, review exposure and resilience, and perform mitigation, recovery, or prevention actions to stop or contain active attacks.

Learn how you can stop attacks through automated, cross-domain security with Microsoft 365 Defender.

Zeev Rabinovich and Ofir Shlomo Microsoft 365 Defender Research Team

Resources

- A practical guide on executing this attack — KrbRelay with RBCD Privilege Escalation HOWTO.
- GitHub Repo of the KrbRelayUp tool that also includes further references.
- GitHub Repo of the original Kerberos Relay attack tool by cube0x0.
- Learn more about Microsoft Defender for Identity, and begin a trial here.
- Learn about Microsoft Defender for Identity's new feature, Response Actions.
- Learn more about Kerberos Constrained Delegation Overview here.