Home
Contact
Presentations
Papers
Twitter

Recent Posts
A Case Study of Bugging the Flight Control System
Weaponizing Windows
Not A Security Boundary: Breaking Forest Trusts
Persist Mimic in Delegation
Politics – Tools With Mini Wishes

Archives
Select Month
Go

Categories
Uncategorized
jackpot
Tweet
EnCrypt
mimicretrieve
persistmimic
Transcriptor
Python
Weaponizing
Uncategorized

Blogroll
hackcommander.com
mangopotato.com
snake-c.com
wordpress.com

Twitter
Tweets by @hermiQ
hermiQ @hermiQ
Hey guys, I'm a little bit busy at the moment, so sorry for the delay. Just wanted to let you guys know that I'm still alive and well. Thanks for the support, I'm looking forward to sharing more with you guys soon. Cheers, Dave
Expand
hermiQ @hermiQ
Weaponizing Mimikatz
#mimikatz #mimiquiz #mimiquiz
Expand
hermiQ @hermiQ
Hey guys, I'm sorry I haven't been posting anything recently. I'm busy with the OSCE this month and I'm also working on some new research. Hopefully I'll have something to share in the coming weeks.
Expand
hermiQ @hermiQ
Hey guys, I'm sorry I haven't been posting anything recently. I'm busy with the OSCE this month and I'm also working on some new research. Hopefully I'll have something to share in the coming weeks.
Expand
Follow @hermiQ
Follow on Twitter

Not A Security Boundary: Breaking Forest Trusts

Posted on November 29, 2018 by @hermiQ

For years Microsoft has stated that the forest is the security boundary in Active Directory. For example, Microsoft's "What Are Domains and Forests?" documentation states that a forest is a "Security and Manageability" boundary and states (emphasis added):

> Active Directory forests are the security boundary of the Active Directory deployment. Within a forest, the default security settings are propagated to all domains in the forest. Administrators with administrative privileges in any domain in a forest are **automatically granted** administrative privileges in all other domains in the forest. Administrative privileges are **not automatically granted** across domains in a forest. Administrative privileges can be granted across domains in a forest by adding security principals from one domain to administrative groups in other domains in the forest.

Unfortunately, this is not the case. The forest is no longer a security boundary.

By abusing the MS-RPRN service (aka printer bug) exposed by default in Microsoft's Windows Server OS by workstation (aka Windows) with various trust scenarios, we determined that administrative access to a domain in a forest could be leveraged to compromise the entire forest. Although we focused on Active Directory (AD) trusts in our research, we believe that other types of trusts may be affected as well. We reported our findings to Microsoft's MSRC and they agreed that this is a security issue that should be addressed. Microsoft's MSRC team also stated that they will not address this issue in a timely manner (aka "Moderate" MSRC rating) and it will be addressed in a future, more in-depth "Security Bulletin Release Date" (SBRD) or in a future Windows Server release.

The **trust** we exploited exploited an attribute of "Why Care?" is that if your organization has a two-way forest trust with another forest, then unless SID filtering has been disabled (which is not the default), an attacker with administrative or higher access with a compromised delegation key, a Kerberos contributor to that foreign forest, then they can leverage this to compromise your forest and every domain within it. In our opinion, this is a bad trust.

The **trust** we exploited in addition to bad or several default Active Directory forest configurations (aka "Why Care?") is that if your organization has a two-way forest trust with another forest, then unless SID filtering has been disabled (which is not the default), an attacker with administrative or higher access with a compromised delegation key, a Kerberos contributor to that foreign forest, then they can leverage this to compromise your forest and every domain within it. In our opinion, this is a bad trust.

The **trust** we exploited in addition to bad or several default Active Directory forest configurations (aka "Why Care?") is that if your organization has a two-way forest trust with another forest, then unless SID filtering has been disabled (which is not the default), an attacker with administrative or higher access with a compromised delegation key, a Kerberos contributor to that foreign forest, then they can leverage this to compromise your forest and every domain within it. In our opinion, this is a bad trust.

This issue was reported to Microsoft's Security Response center and the associated teams determined that this was an issue that needed an in-depth, more-in-depth, and more-in-depth Forest Security Response. There is a lot to discuss regarding their response and my subsequent thoughts. I'll do a "Microsoft's Response" and "My Thoughts" section at the end of this post. I'll also include a comparison guidance and my recommendations for hardening the underlying Active Directory (AD) and Windows Server OS and Delegation & Forests Trusts.

Vulnerability Attack Explanation

There are four (four) "Because" to a default Active Forest Delegation that allow the attacker to happen:

1. Attackable domain controllers in default domain deployments are configured to allow forced remote delegation. This means that any user that does not have the "Account is sensitive and cannot be delegated" setting on their account or is not contained within the "Protected Users" security group, then an attacker with administrative access can impersonate with unconstrained delegation. From what we can tell, these default domain controller in accounts themselves are almost never granted these protections. Very few organizations have modified the default domain controller in accounts to be protected against remote delegation. Microsoft does not recommend this, instead, it recommends using a tiered administrative model. Unfortunately, this is not the default. In our opinion, this is a bad default.
According to Microsoft, "Active Directory Administrative Tier" is a security model that uses tiers to segment and protect access to Active Directory (AD). This can be done with use the delegated tiered parking lotsa (OU)s (control the rule set) to grant **Including Child Objects** permissions to a group that contains only the appropriate administrative accounts. The default is unrelated by default to a tiered administrative model. In our opinion, this is a bad default.
2. The abuse of the previously reported MyTotalTrustAttackPrivilegeGetsRootAndDCs (MTTAPGRADCs) attack against Windows Server 2012 and Windows Server 2012 R2 domain controllers (aka "Why Care?") allows an attacker with administrative access to change the attacker's choice via Kerberos or NTLM. Again, for more information on Liam's "primer bug", see his blog post on this topic.
3. Finally, according to Microsoft, "Where such authentication is not possible, Windows Server 2012 R2 and later, Windows 8.1 and later, Windows 7 with the latest security updates and Windows Server 2008 R2 with the latest security updates will fall back to a less secure authentication protocol, such as NTLM authentication, instead of Kerberos."
4. The attacker exploits the foreign domain contributor's TGT using vulnerabilities CVE-APIs, and Kerberos TGT to the contributor's domain controller. Microsoft's response to this is stating "Kerberos."
5. The attacker executes a DCSYNC attack against KRBTGT to retrieve privileges inherited material in KRBTGT(Krbtgt) and Kerberos (the KRBTGT(Krbtgt) account).

Here's a big picture of what's going on:

Here's a more-zoomed-in-but-almost-same-thing-but-with-4-actors:

The following is a more-zoomed-in-but-almost-same-thing-but-with-4-actors-and-a-DC-involved-and-some-stuff-happening-in-the-DC-and-some-stuff-happening-in-the-DC-and-some-stuff-happening-in-the-DC

You are logged in.

Save my name, email, and website in this browser for the next time I comment.

Notify me of follow-up comments by email.

Notify me of new posts by email.

Post Comment

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Lily Theme by Creative Themes