From DNSAdmins to Domain Admin, When DNSAdmins is More than Just DNS Administration

adsecurity.org

Sean Metcalf October 11, 2018

It's been almost 1.5 years since the Medium post by Shay Ber was published that explained how to execute a DLL as SYSTEM on a Domain Controller provided the account is a member of DNSAdmins. I finally got around to posting here since many I speak with aren't aware of this issue.

Shay describes this issue as follows (bolded text addedby me):

In addition to implementing their own DNS server, Microsoft has also implemented their own management protocol for that server, to allow for easy management and integration with Active Directory domains. By default, domain controllers are also DNS servers; DNS servers need to be reachable and usable by mostly every domain user. This, in turn, exposes quite some attack surface on domain controllers—on one part, the DNS protocol itself and on the other, the management protocol, which is based on RPC.

We will shallowly delve into the protocol's implementation and detail a cute feature (certainly not a bug!) which ***allows us, under some circumstances, to run code as SYSTEM on domain controllers, without being a domain admin****. Although this is certainly not a security vulnerability (so no panic is needed), as confirmed with Microsoft, it's still a cute trick which can be useful as an AD privilege escalation in red team engagements.*

So, how is this possible?
I will summarize Shay's excellent technical review of this issue (this assumes DNS runs on Domain Controllers, which is the most common configuration).

Issue Summary

- DNS management is performed over RPC (UUID is 50ABC2A4–574D-40B3–9D66-EE4FD5FBA076) and the transport mechanism is the \PIPE\DNSSERVER named pipe.
- According to Microsoft protocol specification, the "ServerLevelPluginDll" operation enables us to load a dll of our choosing (with no verification of dll path).
- dnscmd.exe already implements this option:
  dnscmd.exe /config /serverlevelplugindll \\path\to\dll
- When executing this dnscmd.exe command as a user that is a member of DNSAdmins, the following registry key is populated:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\DNS\Parameters\ServerLevelPluginDll
- Restarting the DNS service will load the DLL in this path; however, the DLL needs to contain "one of the DnsPluginInitialize, DnsPluginCleanup or DnsPluginQuery exports."
- So, Shay describes how to modify the DLL in order to load properly and allow the DNS service to start successfully.
- The DLL simply needs to be available on a network share that the Domain Controller's computer account can access.

Keep in mind that Mimikatz includes a DLL that can be customized (since the source on GitHub), so it's possible to update the Mimikatz DLL to be loaded when the DNS service starts and monitor for and dump credentials to a location where the attacker would have access.

Furthermore, Shay notes that DNSAdmins group membership isn't required. It's possible to successfully perform these steps if the account has write access to a DNS server object.

Shay notes that this was reported to Microsoft:

Microsoft's MSRC have been contacted regarding this issue and have stated that it will be fixed by basically only allowing DC administrators to change the ServerLevelPluginDll registry key, and that it will be possible to toggle this feature off in future releases.

Mitigation

- Ensure only admin accounts are members of the DNSAdmins group and ensure they only administer DNS from admin systems. Include DNSAdmins in the list of groups that membership is carefully scrutinized.
- Regularly review the DNS server object permissions for any group/account that shouldn't have privileged access.
- Restrict RPC communication to DCs to only admin subnets.

Reference:

- https://medium.com/@esnesenon/feature-not-bug-dnsadmin-to-dc-compromise-in-one-line-a0f779b8dc83
- http://www.labofapenetrationtester.com/2017/05/abusing-dnsadmins-privilege-for-escalation-in-active-directory.html

(Visited 39,643 times, 12 visits today)