Hunting in Active Directory: Unconstrained Delegation & Forests Trusts

works from an offensive perspective. He also covers specific configurations that you can apply in your environment to potentially help mitigate the attack.

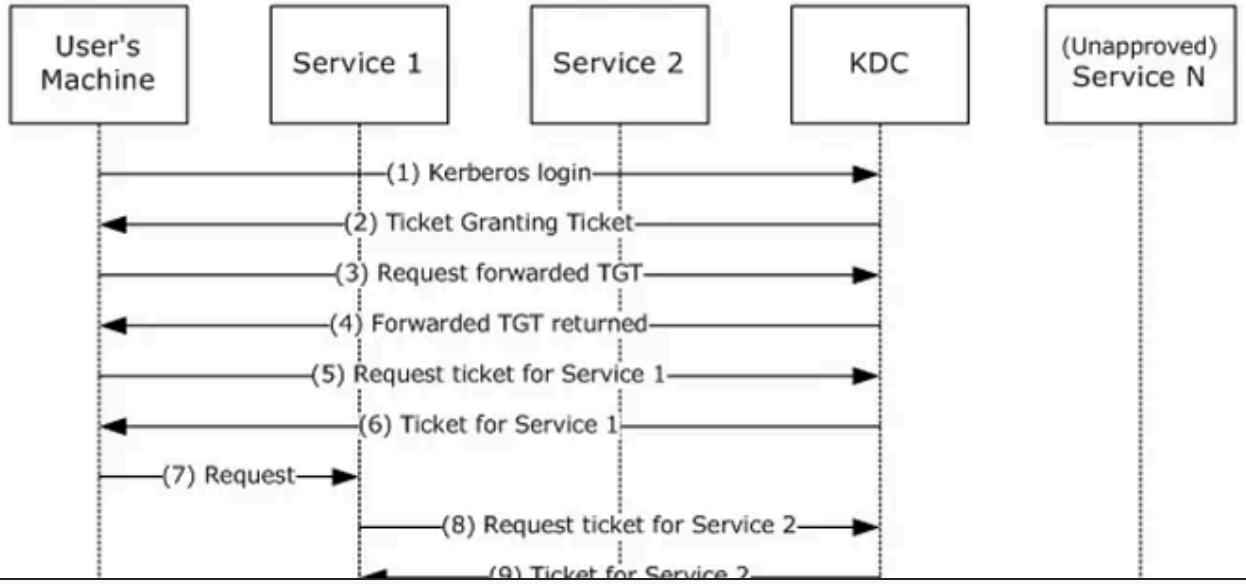
In this post, I will provide initial detective guidance against the attack variation explained in Will's post, focusing primarily on security events generated by the forced-machine-account-auth method in general. I will still provide a few specific indicators of compromise (IOCs) collected from Windows security events generated by Rubeus monitoring for TGTs and the execution of the only publicly available proof of concept code SpoolSample

ticket-granting-ticket (TGT) can be extracted on the attacker-controlled server, reapplied, and used to compromise the credential material in the foreign forest."

Understanding the Concepts Applied in the Attack

Before we start simulating and documenting the detection of this attack, it is very important to understand what the attacker does and why. In this section, I will provide several of the articles and documentation that helped me understand the attack a little bit better. A few things that stood up for me about the attack from Will's post were the following:

Delegation	Delegation Style	Description
Unconstrained	TGT Forwarding	When a user accesses a server with unconstrained delegation enabled, the user sends their TGT to the server. The server can then impersonate the user by using the user's TGT to authenticate to other services in the network.
Traditional Constrained	Service for User to Self (S4U2self) Service for User to Proxy (S4U2proxy)	Any accounts (user or computer) that have service principal names (SPNs) set in their **msDS-AllowedToDelegateTo** property can pretend to be any user in the domain (i.e. they can "delegate") to those specific SPNs.
Resource-Based Constrained		Implemented with a security descriptor on the target resource, instead of a list of SPNs on the "frontend"



5. The user makes a request for a service ticket to Service 1 using the TGT returned in step 2. This is done by the KRB_TGS_REQ message.
6. The ticket-granting service (TGS) returns the service ticket in a KRB_TGS_REP.
7. **The user makes a request to Service 1 by sending a KRB_AP_REQ message, presenting the service ticket, the forwarded TGT, and the session key for the forwarded TGT.**
8. To fulfill the user's request, Service 1 needs Service 2 to perform some

15. Service 1 can then continue to impersonate the user with Service N. This can pose a risk if, for example, Service 1 is compromised. Service 1 can continue to masquerade as a legitimate user to other services.
16. Service N will respond to Service 1 as if it was the user's process.

The server, with unconstrained delegation configured, can ultimately use the forwarded TGT not only to access other non-requested services in the network, but to execute attacks such as DCSync if it is a Domain Controller TGT. You can read more about the details provided above in here. As you

When a new domain is added to the root domain, two-way transitive trusts are created by default.

RpcRemoteFindFirstPrinterChangeNotification(Ex) method to force any machine running the Spooler service to authenticate to a target of the attacker's choice via Kerberos or NTLM.

What is the [MS-RPRN] Print System Remote Protocol?

According to Microsoft Docs, it is based on the Remote Procedure Call (RPC) protocol that supports synchronous printing and spooling operations between a client and server, including print job control and print system management. In addition, the Print System Remote Protocol uses RPC over

server) is all it takes for the "printer bug" to work. When the RpcOpenPrinter method is executed, it needs to return an ERROR_SUCCESS value to jump to the notification method which is expected to fail with specific nonzero return values. Lee's POC monitors for the two following return ERROR values and provides the following messages:

- **ERROR_ACCESS_DENIED:** "*Target server attempted authentication and got an access denied. If coercing authentication to an NTLM challenge-response capture tool (e.g. responder/inveigh/MSF SMB capture), this is expected and indicates the coerced authentication worked*"

Domain Controller (DC) of the root domain and used it against another DC in a separate forest.

A victim forest

- A Domain Controller (**rikers.cyberpartners.local**) as the victim since we want its TGT to then perform a DCSync attack from the compromised DC with unconstrained delegation configured.

Account localadmin in **hydrogen.covertius.local** requests a Kerberos service ticket with SPN **CYBERPARTNERS.LOCAL** to connect over to the other forest. Kerberos auth happens because SpoolSample uses the DNS name of the server and not its IP address.

rikers$ was forced to authenticate to our server with unconstrained delegation configured.

The named pipe share named IPC$ is accessed on **hydrogen.covertius.local** by **rikers.cyberpartners.local** in order to bind to the **spoolss** service on the client. Something to point out is that the account accessing the IPC$ is our localadmin from COVERTIUS and not **rikers$ (delegation)**

step fails, then it could be that the user running rubeus might not have the proper privileges to get a handle to LSA. That's exactly what happens:

was mean to document the security events generated during the main steps of the attack presented in Will's post.

Initial Detection Recommendations:

Rubeus

- Rubeus was executed on disk for this proof of concept so you can build a basic signature based on the command line arguments. Keep in mind that command line values have a high attacker influence rating, which means that the command arguments can be manipulated by the attacker

This specific variation of the attack forces **Domain Controllers** to authenticate to a compromised server with unconstrained delegation configured over a two-way forest trust. Therefore, as we saw in this sequence of events, expect **SID filtering** events (**Security event 4675**) on the unconstrained server with **filtered SIDs matching Enterprise Domain Controllers (S-1–5–9).**

- Get a list of servers with unconstrained delegation configured and stack each instance of **Security event 4675.**

spoolss service over IPC$ from unconstrained server covers just this implementation of the attack.

. . .

I hope this post was helpful for those that just read about the awesome "Not a Security Boundary: Breaking Forests Trusts" blog post from my teammate Will, and wanted to learn more about most of the data generated at the endpoint level when the attack is executed. This post covered only one

https://www.harmj0y.net/blog/redteaming/another-word-on-delegation/

https://msdn.microsoft.com/en-us/library/cc246071.aspx

https://www.harmj0y.net/blog/redteaming/a-guide-to-attacking-domain-trusts/

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc775736(v=ws.10)#trust-types-1

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)#forests-as-security-boundaries

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc755427(v=ws.10)

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn745899(v=ws.11)

Written by Roberto Rodriguez

1.6K Followers · Writer for Posts By SpecterOps Team Members

Follow