Detecting domain trust discovery attempts

Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain, allowing the users of the trusted domain to access resources in the trusting domain. Attackers may attempt to perform domain trust discovery as the information they discover can help them to identify lateral movement opportunities in Windows multi-domain/forest environments.

Domain trusts can be enumerated using the DSEnumerateDomainTrusts() Win32 API call, .NET methods, and LDAP. The Windows utility Nltest is known to be used by adversaries to enumerate domain trusts.

These searches look for activity consistent with attackers attempting to perform domain trust discovery.

Required data

Endpoint data

Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

How to use Splunk software for this use case

► Windows adfind.exe execution

To complete this process, your deployment needs to ingest logs with the process name, and command line executions from your endpoints. If you are using Sysmon, you must have at least version 6.0.4 of the Sysmon TA. You should also ensure you are ingesting normalized endpoint data, populating the Processes node of the Endpoint data model in the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

This search looks for the execution of adfind.exe with the filter or search command line arguments that it uses by default. It also considers the arguments necessary like objectcategory. Adfind.exe is rarely used by administrators for legitimate reasons so you should investigate any results that are returned from this search.

Dsquery domain discovery

To complete this process, your deployment needs to ingest information on process that include the name of the process responsible for the changes from your endpoints. You should also ensure you are ingesting normalized endpoint data, populating the Processes node of the Endpoint data model in the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

This search looks for dsquery.exe execution with arguments looking for a TrustedDomain query on the command line, which indicates domain trust discovery is being performed.

This search does not identify any other variations of dsquery.exe usage. Within this search, it is assumed that dsquery.exe is not moved or renamed. The search will return the first time and last time these command line arguments were used for these executions, as well as the target system, the user, process "dsquery.exe" and its parent process.

Dsquery.exe is natively found in C:\Windows\system32 and C:\Windows\syswow64 and only on server operating systems. Dsquery.dll is loaded when DSQuery.exe is launched. If you find this DLL loaded by another process, it is possible dsquery is running within that process context in memory.

When reviewing any results from this search, you should review parallel processes for additional behaviors performed, as well as identifying the parent process and capturing any files being used, for example, batch files.

Nltest domain trust discovery

To complete this process, your deployment needs to ingest information on process that include the name of the process responsible for the changes from your endpoints. You should also ensure you are ingesting normalized endpoint data, populating the Processes node of the Endpoint data model in the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

This search looks for the execution of nltest.exe with command line arguments used to query for domain trust information. /domain trusts returns a list of trusted domains, and /all_trusts returns all trusted domains. Attackers use nltest.exe to enumerate the current domain, which helps them understand where to pivot next.

---

### Next steps

The content in this article comes from [Splunk Enterprise Security (ES)](https://www.splunk.com). As a Splunk premium security solution, ES solves a wide range of security analytics and operations use cases including continuous security monitoring, advanced threat detection, compliance, incident investigation, forensics and incident response. Splunk ES delivers an end-to-end view of an organization's security posture with flexible investigations, unmatched performance, and the most flexible deployment options offered in the cloud, on-premises, or hybrid deployment models. If you have questions about this use case, see the Security Research team's [support options on GitHub](https://github.com/splunk).

In addition, these Splunk resources might help you understand and implement this use case:

- E-book: [Ransomware, malware and cyberthreats](https://www.splunk.com)
- Blog: [Hunting with Splunk: The basics](https://www.splunk.com)

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.