Black Lantern Security (BLSOPS)

Subscribe Sign in

DETECTION ENGINEERING

Detecting DCSync

Understanding and Detecting MITRE T1003.006 - OS Credential Dumping: DCSync

BRIAN O'HARA
DEC 04, 2020

Share

Introduction

A common favorite “domain domination” technique for Black Lantern Security (BLS) operators during engagements is to perform a DCSync attack to obtain all the juicy credentials they can acquire. Because this technique generally flies under the radar of detection and logging capabilities at most organizations, the first question from the client during outbrief always seems to be, “*How did you do it?*” In an effort to aggregate many of the community resources, research, and shared experience and to demystify some of this technique’s nitty gritty technical details in a digestible manner for our clients, we have put together a brief write up.

Overview

The DCSync attack methodology takes advantage of the Directory Replication Service Remote (DRSR) protocol to obtain sensitive information from a domain controller. [1] This technique involves an adversary masquerading their host as a domain controller (DC) and convincing the authentic DC to synchronize its database to the new rogue DC by issuing a replication request. This functionality is not a bug, but rather is intended activity to provide user friendly redundancy in a multi-DC network. The attack does require elevated privileges to complete. The user account used to perform the data replication request must have the ”replicating directory changes” privilege, environment. The recommended deployment configuration from Microsoft suggests including more than one DC for redundancy and load balancing purposes. [3] As this is the advice given directly from the vendor, it is likely to be encountered in many corporate networks and all but guarantees ongoing replication activity. The fact that replication behavior is expected makes detection of “malicious” activity very challenging on a flat network. The sheer volume of alerts from a flat network will eventually cause alert fatigue and many times the results of an investigation will end up being legitimate activity. By implementing proper network segmentation, DRSR protocol activity is limited to the DC VLAN and detective measures can be put in place so that the IDS/IPS signatures only alert on attempts to replicate the DC database *outside* of the controlled DC segment. In this configuration, preventative controls may also be put in place as well to block DRSR traffic that is routed outside of the DC network segment.

Example Suricata signatures created by Didier Stevens research can be seen below. [4]

```
alert tcp !$DC_SERVERS any -> $DC_SERVERS any (msg:"Mimikatz DRSUAPI";
flow:established,to_server; content:"|05 00 0b|"; depth:3; content:"|35 42 51
e3 06 4b d1 11 ab 04 00 c0 4f c2 dc d2|"; depth:100; flowbits:set,drsuapi;
flowbits:noalert; reference:url,blog.didierstevens.com; classtype:policy-
violation; sid:1000001; rev:1;)

alert tcp !$DC_SERVERS any -> $DC_SERVERS any (msg:"Mimikatz DRSUAPI
DsGetNCChanges Request"; flow:established,to_server; flowbits:isset,drsuapi;
content:"|05 00 00|"; depth:3; content:"|00 03|"; offset:22 depth:2;
reference:url,blog.didierstevens.com; classtype:policy-violation;
sid:1000002; rev:1;)
```

Note that both signatures are inspecting for traffic originating from any network segment that is NOT the DC segment and that includes calls to drsuapi through RPC/DCE traffic. The first signature is looking for a bind event, which is a required prerequisite to call individual functions from the DRSUAPI. The second alert is specifically targeting the flag associated with DsGetNCChanges requests. Both enabled by default and must be explicitly configured. Based on the Microsoft documentation, the decision to omit these events from default logging was based on the high volume of logs that can be generated. For example, event ID 4662 will be created for any access attempts to a directory service object in which a security access control list (SACL) has been assigned. 4662 events are also generated when access to the WMI namespace, *MicrosoftVolumeEncryption*, is referenced. [6] When Bitlocker is enabled in the environment, this generates substantial log volumes and has been cause for many organizations to eventually disable the event after initial configuration. One final recommendation is to NOT enable failure auditing as these event logs are infamous for flooding log collectors in the 10+ million range when a single error occurs.

This event log correlation method, like the network detection method, also requires some prerequisite planning steps. For this method of detection to be efficient and to facilitate effective rule tuning, a strong baseline of legitimate replication activity should be identified.

Investigating Using a SIEM

From a SIEM alerting perspective, if the host names of the DCs are known and documented, their machine account names can be explicitly omitted from security event generation as that is expected behavior. Another way to limit the volume of logs from these events (at least from the SIEM perspective) is to implement a blocklist on the event forwarder so that only 4662 events of interest are captured and transferred to the centralized logging platform. This process and implementation will vary depending on both the log forwarder and the SIEM, and will require tailored research.

An example where the forwarder was tuned within the BLS Detection Lab is detailed below (**Note:** this is not specific to DCSync detection): [7]

> The blacklist feature of the Splunk Universal Forwarder v6.1+ can be utilized to filter events. An additional line would need to be placed in

Sample 4662 Event Log from a Successful DCSync Attack

For authentic replication activity the "**SubjectUserName**" should contain the name of the machine account of a domain controller or a variation of NT AUTHORITY/SYSTEM. This data field will need to be evaluated within the target environment that is being monitored. What is shown here is only an example. For this detection method, any logs that match the additional criteria listed below and include a regular user account in the "**SubjectUserName**" field, should be investigated further.

3. {**9923a32a-3607-11d2-b9be-0000f87a36b2**} - DS-Install-Replica 4.*{89e95b76-444d-4c62-991a-0facbeda640c} - DS-Replication-Get-Changes-In-Filtered-Set

It is important to note that within the community there is some disagreement with regard to the presence of the GUID versus the more generalized statement ("**Replicating Directory Changes all**") that's captured in these logs. At this time, it is recommended to enrich the detection criteria to search for either the GUIDs or the replication statement to capture all possible scenarios. While hunting client environments for this type of activity, BLS has found this string instead of the GUIDs above.

Benjamin Delpy (@gentilkiwi), the researcher who discovered and pioneered the DCSync attack technique, has also provided a few recommended Splunk queries to hunt for this activity. [11] Some of his searches have been found to be a bit generic when utilized in larger corporate environments and may produce overwhelming results. However, one of the suggestions he makes that could prove useful in tuning efforts is to exclude events where the SubjectUserSID includes "AUTHORITE NT". This may be something to consider should the other criteria above overwhelm the Logs/SIEM with large numbers of events.

Note: For those curious about the other GUID seen in the log example above, "*{19195a5b-6da0-11d0-afd3-00c04fd930c9}*", this is associated with the RPC function: WRITE_DAC. Though this will be present in each of these event logs, it is not very helpful in detecting DCSync activity specifically. This is a standard access permission to modify discretionary access control lists in an object's security descriptor.

After testing using the BLSOPS lab environment, we were able to efficiently detect this activity successfully using the explained log criteria.

Lab Sample Splunk Query:

index=main EventCode=4662 Access_Mask=0x100 AND ("Replicating Directory Changes all" OR "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2" OR "1131f6aa-9c07-11d1-

[1] https://adsecurity.org/?p=1729

[2] https://adsecurity.org/?p=1729; https://blog.didierstevens.com/2017/10/08/quickpost-mimikatz-dcsync-detection/

[3] https://social.technet.microsoft.com/Forums/windowsserver/en-US/991d4f68-5178-4c9a-8b7d-8f2b5f53867e/how-many-domain-controllers-are-recommended?forum=winserverDS

[4] https://blog.didierstevens.com/2017/10/08/quickpost-mimikatz-dcsync-detection/

[5] https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-directory-service-access

[6] https://static1.squarespace.com/static/552092d5e4b0661088167e5c/t/5c58669615fcc0dce4024cc1/1549297303121/Windows+Advanced+Logging+Cheat+Sheet_ver_Feb_2019_

[7] https://www.splunk.com/en_us/blog/tips-and-tricks/controlling-4662-messages-in-the-windows-security-event-log.html

[8] https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4662

[9] https://social.technet.microsoft.com/Forums/windows/en-US/541bad5d-19eb-4de5-8ef7-1b144f0b6113/translate-xxxx-values-in-events?forum=w7itprosecurity

[10] https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/1522b774-6464-41a3-87a5-1e5633c3fbbb; gist.github.com/gentilkiwi/dcc132457408cf11ad2061340dcb53c2#file-dcsync-dcshadow-splunk

[11] gist.github.com/gentilkiwi/dcc132457408cf11ad2061340dcb53c2#file-dcsync-dcshadow-splunk

Black Lantern Security (BLSOPS)

Timely research, discussion, and tactics for Cybersecurity leadership, operators, and analysts.

Type your email... Subscribe

♡ 💬 ⟳ Share

Discussion about this post

Comments Restacks

Write a comment...

Top Latest Discussions

Subdomain Enumeration Tool Face-off 2022

Comparing the industry's top subdomain enumeration tools

OCT 12, 2022 • THETECHROMANCER

Detecting LDAP Recoannaissance

Techniques to Identify Active Directory Enumeration

JUN 28, 2021 • ADEEM MAWANI

Introducing TREVORproxy and TREVORspray 2.0