DETECTION ENGINEERING

Detecting DCSync

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

BRIAN O'HARA

DEC 04, 2020

Share

Introduction

the data replication request must have the "replicating directory changes" privilege, which is commonly found associated with administrator and domain administrator credentials. The results of a successful DCSync attack will provide the adversary with password hashes of the targeted users. In most cases, this will include all users.

Detection on the Wire

The security community's current recommendation for detecting a DCSync attack is to implement a detection signature at the network layer (typically through an IDS/IPS application) to identify RPC/DCE traffic, which includes calls to the DRSUAPI RPC interface. [2] Network layer detection has proven to be the most consistent and easiest way to detect this type of attack. The detection criteria can be further customized to 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;
```

enabling “*Audit Directory Services Access*” through Group Policy (*Computer configurations > Windows Settings > Security Settings > Local Policies > Audit Policy > Audit Directory Service Access > Enable Success)*. [5] By configuring this setting, two new event IDs will be generated in the logs: 4661 and 4662. Each of these event IDs can be viewed in the Security log using the standard Event Viewer application. Both of these events are extremely generic and track access attempts to directory service objects. The 4662 event ID generated by DCSync activity is specifically targeting actions where, *“An operation was performed on an object*”. It is important to note that this event ID is not 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 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 *Splunk_TA_windows\local\inputs.conf* and pushed to the DCs.

A Legitimate Replication Log Example

The “**AccessMask**” captured in the event log should be **0x100**. [8] This value represents “control access” and is specifically registered when access is allowed following extended rights verification (typically associated with the use of high level and explicit permissions that are required to initiate the DCSync attack).

The “**Properties**” field will include 2 pieces of relevant information to search for. The first is the starting string in the log example above, “**%%7688**”. [9] This is another flag that is assigned and is associated with “Control access”. The second is the long string of characters at the end of that field, which are registered GUIDs that represent each

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:

Splunk Search Example

Share

[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

Discussion about this post

Comments Restacks