Monday, January 30, 2017

Hunting: What does it look like?

It's been a while since I've posted anything and wanted to get this out. Partly because of an article that I read that talks about how attackers may move laterally within your network. The other reason is because I think it really shows what you can do with windows event logs (provided you have certain logging enabled) to identify anomalous behavior.

We know that attackers will often use built-in operating system utilities to facilitate host/user enumeration and lateral movement (if you want to dig more into what I will be talking about I would suggest starting here https://attack.mitre.org/wiki/Discovery). I have previously made the recommendation that if you have command line process auditing enabled to focus much attention on the system32/syswow64 directories. Looking for rare or fist seen command line arguments from processes that are spawned from these directories can, at times, point to malicious behavior when lateral movement is involved. If attackers have brought tools in with them to facilitate enumeration or lateral movement this method can become much more difficult as the command line arguments may be unknown and simply glossed over. If we flip this around though and look at effects of enumeration on the destination side we may be able to spot what may have otherwise been missed.

I am a big advocate of looking for the same things multiple ways and in different log sources. There are times where logging events fail due to network issues, application issues… Having layers of coverage is a good idea, imho, and this includes trying to identify the same activity on both source and destination machines.

Now for the article which you can read here: https://blogs.technet.microsoft.com/enterprisemobility/2017/01/24/cyber-security-attackers-toolkit-what-you-need-to-know/. The author does a good job of describing some of the tools and methods that may be employed by an attacker, but falls short when it comes to discussing how to find indications of this behavior. Instead they make the statement "With an assumed-breach mindset, we assume the attacker has already breached the perimeter and is on the network. Unfortunately, this is when the adversary goes dark to the defender, as the attacker has already breached network defenses as well as antivirus." If you have the necessary logging enabled, I don't believe they need to go dark.

If we dive into what they describe they first talk about the "net user" and "net group" commands. How might these look to a defender?

Source:
net user administrator /domain
Destination:
Event Code: 4661
Object Type: SAM_USER
Object Name: S-1-5-21-*-500 (* represents domain)
Access Mask: 0x2d
Note: In my testing, users in the Domain Admins group will display a SID. Other users will not. The exception is the Guest and krbtgt accounts. I would also pay attention to the krbtgt SID S-1-5-21-*-502. I would think that it would be very odd to see this and may indicate an attacker is intending to use Golden Tickets.

Object Name: S-1-5-21-*-512
Access Mask: 0x2d

Note: Also pay attention to the Enterprise Admins group with the SID of S-1-5-21-*-519

The following can be used to identify PowerSploit's Get-NetSession, Get-NetShare, netsess.exe and net view. The net view command may look something like "net view \\192.168.56.10".

Destination:
Event Code: 5145
Relative Target Name: srvsvc
Share Name: IPC$
Access_Mask: 0x12019f

Note: These events may be very loud. I would suggest looking for a single source creating srvsvc pipes on multiple machines within a specified time frame. This may be indicative of enumeration activity.

The article goes on to talk about the use of mimikatz and the use of hashes and kerberos tickets.

One method I have found to identify an attacker obtaining hashes through lsadump is to look for the following. I have also found this to be a pretty accurate indicator and would suggest, if you have these logs, to monitor for this event.
Event Code: 4656
Object Type: SAM_DOMAIN
Process Name: lsass.exe
Access Mask: 0x705

For kerberos ticket theft, I have not found an accurate way to identify this in the event logs, but when executed with mimikatz there will be files written with the .kirbi extension. If an attacker was using WCE there would be two files created named wce_ccache and wce_krbtkts. These files can obviously be renamed, but If you have the ability to monitor file creations I would recommend including all of these and hopefully catch when they are dropped on the file system and before renaming.

With respect to the article, I would like to thank Microsoft for putting it out. I believe that more should release what attackers are doing so that people can focus attention to what is being used. I see a lot of threat hunting providers say you need it, but don't share any of what they look for or why they look for it. I hope those that do this choose to share more in the future.

I would love to hear what others are doing with regards to hunting for and detecting the above. Finding innovative ways to hunt for bad guys is what I'm passionate about so please share in the comments section.

Posted by Jack Crook at 9:20 AM

4 comments:

Anonymous January 30, 2017 at 4:16 PM

good stuff, thanks! could you also share the article you mention on the first lines ?

Reply

Replies

Jack Crook January 31, 2017 at 3:09 AM

Jack,

> "I would love to hear what others are doing with regards to hunting for and detecting the above"

are you familiar with the Threat Hunting Project and its "hunts" repo?
http://www.threathunting.net/
https://github.com/ThreatHuntingProject/ThreatHunting/tree/master/hunts

Cheers,
Tom

Reply

Jack Crook January 31, 2017 at 9:41 AM

Hey Tom,

Thanks for the comment. Yep, I've posted several hunts there and IIRC you even used one in a presentation of yours. :)

Reply

Note: Only a member of this blog may post a comment.

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)