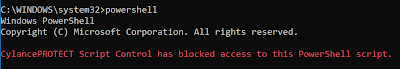
**Intro to Next Generation Antivirus**

As a security professional, Cylance and I have very much what you'd call a love-hate relationship.  Since Cylance uses math and algorithmic based detection and doesn't rely on signatures as it's predecessors did, it does an excellent job at identifying and preventing malware from executing.  Carbon Black and Endgame are just a couple of others on the market today.  These next-gen AV products are quickly picking up pace as I notice more and more of our penetration testing customers leveraging these solutions in their enterprise environments.  That's great!  Right?..  Well, depends on who you're asking.

As a red teamer it can be quite frustrating when custom backdoors, which score a zero on VirusTotal by the way, are now being detected and blocked by these next generation products.  Uncool!  So what can we do?  Let's disable it altogether.. that'll show.. them?  Always a tricky situation when we recommend a product but we're able to demonstrate how we bypassed said recommended solution.  I want to share a recent experience during a penetration test where I encountered a Cylance PROTECT agent we previously sold to our customer, the issues I ran into, and the solution I came up with.

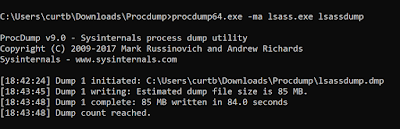
**Gaining Access to a Windows Machine**

I'm going to assume you just gained access to a Windows box.  In my case, I manually exploited CVE-2017-12149 and landed as a Local Administrator with a shell on a Win 2008 R2 server.  Great!  This will be easy.. I'll just paste my Empire launcher in and get an agent on the other side with elevated privileges.  Not so fast.. the stager isn't completing but telnet is telling me traffic can exfil out to my listener.  What gives?  You guessed it... ***CYLANCE!*** 😒  Cylance not only blocked my Powershell launcher but wouldn't even allow me to Invoke-Mimikatz to dump creds.  Booo!

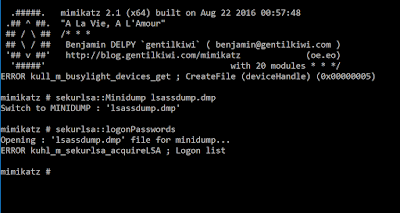
[](https://2.bp.blogspot.com/-KTC7Xeilajk/W2pBXky0HXI/AAAAAAAAM1w/lF1si4eL7g4L2zQqNG9h9Bdx8xoI4iozgCLcBGAs/s1600/WhoAmI%2BSYSTEM%2BBlock%2BPowershell%2BScript%2BExecution%2B-%2BCopy.PNG)

**CylancePROTECT Script Control has blocked access to this PowerShell script**

Oh well, I'll just load ProcDump (a Microsoft signed binary) to bypass AV and dump the lsass.exe process for offline parsing with Mimikatz and get those precious credentials that way!  WRONG.  Apparently Cylance interferes in a way that seems to corrupt the mini dump so I can't parse it with Mimikatz on another machine.

[](https://2.bp.blogspot.com/-BESRwxh7lEU/W2o-HlFWytI/AAAAAAAAMzw/4SkkgrSkfk0gKbKcNm4cAd2d0WnLRzGrQCLcBGAs/s1600/LSASS%2BProcDump.PNG)

**procdump -ma lsass.exe lsassdump**

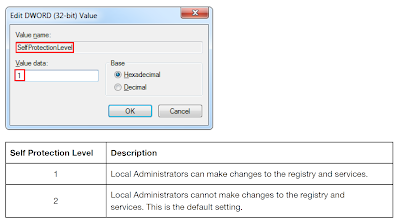
[](https://1.bp.blogspot.com/-gWVzLeNne04/W2o-Ie58vDI/AAAAAAAAMz8/4t6nvRGGwsEXuLanXgIyTftZuLHJQ1u0wCLcBGAs/s1600/Mimikatz%2BFailure%2BWhen%2BLSASS%2BAcquired%2Bby%2BSYSTEM%2Bw%2BCylance.PNG)

**ERROR kuhl\_m\_sekurlsa\_acquireLSA ; Logon list**

Que?  After what seemed like hours of troubleshooting possible permission and architecture issues, I went down the route of trying to load the mimilib.dll file into a debugger but was finding it couldn't locate the lsass.exe process within the dump.  I also later tried with elevated "SYSTEM" privileges with the same fate.  That's when it it finally dawned on me that Cylance may have been interfering with the dump and corrupting the file somehow.

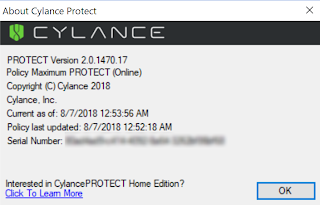
**Killing Cylance**

Ok, so I just have to kill Cylance now right?  That won't be easy, especially since I know Cylance supposedly has the "Self Protect" service option that we as customers have been told is "Impossible to Kill".

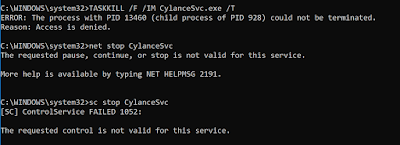
[](https://2.bp.blogspot.com/-HWv1lM5vPkY/W2pCyS_MobI/AAAAAAAAM18/hhQQlm9oWuwtpmCITzCGFwnCqTufMaCygCLcBGAs/s1600/Cylance%2BSelf%2BProtect%2BRegistry%2BSettings.PNG)

**Cylance SelfProtectionLevel Settings via the Installation Guide**

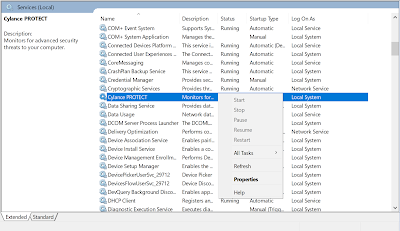
And sure enough, as I'd expect, I can neither stop the CylanceSvc service nor kill the CylanceSvc.exe process in my local administrator context.  Let's create a local admin account and add myself to the "Remote Desktop Users" group so I can at least see what's going on here.

[](https://3.bp.blogspot.com/-ISmfnMm_Dv8/W2pEUod-bOI/AAAAAAAAM2I/2Sw6rcYhcN4aqTE1wsBSnxFjlV0DwsMhwCLcBGAs/s1600/Cylance%2BClient%2BMaximum%2BProtect.PNG)

**Maximum PROTECT**

[](https://1.bp.blogspot.com/-Pyumas6l9b8/W2pGNa2XsvI/AAAAAAAAM2U/1NGPFfjvJVYX20yIwqtShWW7KKZKzPyxwCLcBGAs/s1600/LocalAdmin%2BCant%2BStop%2BCylance.PNG)

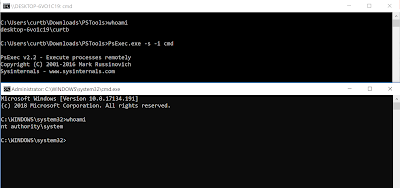
**Failure to Kill Task via "sc" and "net" Commands**

[](https://1.bp.blogspot.com/-W_yYn6llwtY/W2o-IZIY2cI/AAAAAAAAM1Q/FWhlf0sR3MESM3kookv2UyV1FEIiHOvYgCEwYBhgL/s1600/Grayed%2BOut%2BServices.msc.png)

**Grayed-out Service Status Options**

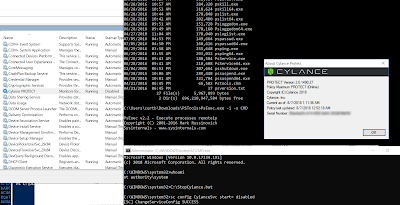
My agent's policy is set to **Maximum**and I'm unable to stop the process or service via the command line or GUI.  However, I know that the Cylance Service is running with privileges higher than that of a Local Admin, so it's time to use some privilege escalation techniques to acquire "SYSTEM" rights.

Because most post-exploitation techniques require tools or a backdoor in memory (*like MSF's "getsystem" or PS Modules like PowerUp, etc*) to easily elevate privileges, I'll have to avoid those since Cylance won't allow them to even touch disk, let alone execute.  Because I'm a fan of using good tools for bad, and because it's another MS signed binary, I opted to load our old friend PsExec from PsTools on the box.  As a local administrator, I could easily run "***PsExec.exe -i -s cmd"*** from an elevated command prompt (run as administrator) to get that "SYSTEM" delegation I was going for.

[](https://2.bp.blogspot.com/-B5Ay2LrFHXM/W2pJEidlYDI/AAAAAAAAM2g/uhyHqiJS1-cmYkw9yxg5BiFv6x_B3IvEACLcBGAs/s1600/Priv%2BEscalation.PNG)

**Using PsExec to Elevate from Local Admin to SYSTEM**

And Yes, to answer your question, this technique ***still*** works in 2018 on Windows 10... Let's not go there. 😮 But hey, alright!  Surely since we're SYSTEM now we can shut down that pesky Cylance process and service right?  After all, it's running as SYSTEM itself according to services.msc.  NOPE! <insert nope meme here>

[](https://2.bp.blogspot.com/-cXY6fzobzPA/W2pONCwnkWI/AAAAAAAAM2s/_xRtMNUwsxIdofkCAEJ6PxB-U2zVcxv-wCLcBGAs/s1600/PsExec%2Bto%2BSYSTEM%2BThen%2BDisable%2BCylance%2BNewest%2BVersion.PNG)

**Successfully Disabled Service via SYSTEM with "sc config CylanceSvc start= disabled"**

Well, not quite anyways.  With SYSTEM access I found I can now actually disable the "Startup Type" for the service from "Automatic".  I can't, however, kill that pesky process.  ***Error: The process could not be terminated.  Reason: Access is denied.***So what?!  This is what I've been looking for!  I can now bounce the box and when it comes back online Cylance won't be running and that box will do my bidding!  But.. as a penetration tester I know that my cached credentials will go along with it.  I need to kill the process somehow but what can I do when SYSTEM can't even force terminate the CylacneSvc.exe PID?

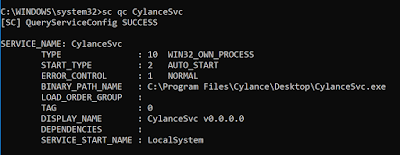
**Bringing it Home**

I'll spare you all of the various ways I went about (***and FAILED***) at killing the process.  Okay! ..so they involved impersonating TrustedInstaller tokens, using elevated Process Explorer & Resource Hacker tools, killing process handles, and injecting junk into the process to cause corruption and die.  Now, let's talk about what ***DID*** work, and boy was it simple in the end.

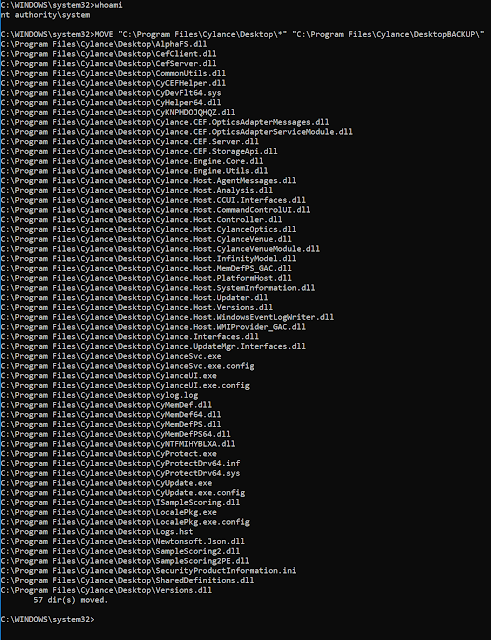
It turns out the SYSTEM user (not an Admin) can move the Cylance binaries that are loaded in memory, on disk to another location.  I discovered that doing so instantly causes the process to keep running but stop functioning until the moment they're moved back.  Strings told me it's set to ignore errors and just keep on keep'n on.  Let's demonstrate:

[](https://3.bp.blogspot.com/-hE6XzVgk7dQ/W2o-RVrcoSI/AAAAAAAAM1U/iDz1ODxBgk4UQUn45Ci-WHPhxnMMzHk-wCEwYBhgL/s1600/WhoAmI%2BSYSTEM%2BBlock%2BPowershell%2BScript%2BExecution.PNG)

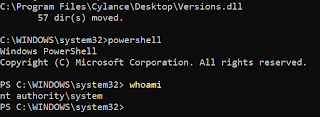
**Still no Powershell Execution as SYSTEM**

[](https://3.bp.blogspot.com/-xxocdyxmQlc/W2o-L8B3bZI/AAAAAAAAM1o/d_fsqQZlvFMoJi7PHWUuVJsObyqdhPyUgCEwYBhgL/s1600/Service%2BQuery%2BCylance%2BService%2Bfor%2BPath%2BInfo.PNG)

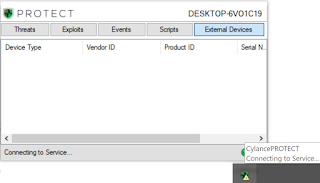
**Locating the CylanceSvc Path via "sc qc CylanceSvc"**

[](https://4.bp.blogspot.com/-VQTn09MHeqg/W2pPPyF7_jI/AAAAAAAAM20/zpO4m5Oq7QsTTO3BcYuDPui0sLrKnvKPACLcBGAs/s1600/Moved%2BFiles.PNG)

**MOVE "C:\Program Files\Cylance\Desktop\\*" "C:\Program Files\Cylance\DesktopBACKUP"**

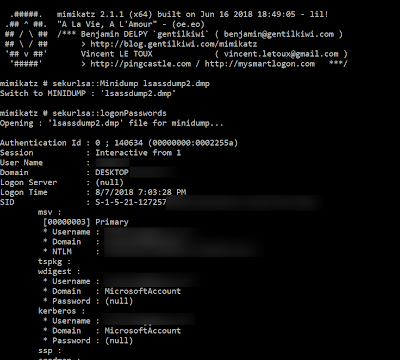
[](https://1.bp.blogspot.com/-pU65vC2cexE/W2pQiGnzczI/AAAAAAAAM3A/uWT4o3mH0zo0xVJ65wGNLh9nqwObdOcGwCLcBGAs/s1600/PowerShell%2BWorking.PNG)

**PowerShell, it's ALIVE!!**

[](https://1.bp.blogspot.com/-Tfg62pZ1_WE/W2o-BShLIvI/AAAAAAAAM1o/m9QEamypwNMASku2jJqfLjt-J4PUBJUPACEwYBhgL/s1600/Cylance%2BAgent.png)

**Cylance PROTECT No Longer Connecting to Service**

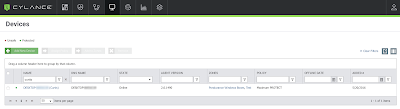
Woo hoo!  Time to celebrate!  I can now execute any payload I'd like to and Cylance is just sitting in the corner drooling on itself.  Let's try Mimikatz one more time to ensure Cylance was the culprit earlier:

[](https://4.bp.blogspot.com/-t31MEbLc5iQ/W2pRpVGxlBI/AAAAAAAAM3I/5PtPXX4I25AloVpr43QL9Bt933XSL8MGQCLcBGAs/s1600/Mimikatz%2BLocal%2BLSASS%2BWorking%2BAfter%2BKilling%2BCylance%2BHandles.PNG)

**With Cylance "Disabled" Mimikatz Runs and Returns Credentials Again!**

**(So do my Empire launchers)**

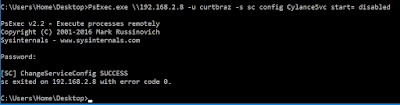
 Oh, and don't forget to move your files back when you're done with a simple ***MOVE "C:\Program Files\Cylance\DesktopBACKUP\\*" "C:\Program Files\Cylance\Desktop\"***.

[](https://3.bp.blogspot.com/-uTHFFtbkOVo/W2pTyekXa1I/AAAAAAAAM3c/rU62tdxbGp4Wdq67jzLh2VONOOvZxN73gCLcBGAs/s1600/image%2B%252816%2529.png)

**Instantly Back Online Again (From the Admin Console)**

**Closing Thoughts**

I hope you enjoyed the journey with me!  I did.. after it was over.  During, I pulled some hair out (*my own*), screamed, almost threw my laptop, and celebrated a few victory dances in the early morning.  I'm sure there's more than one way to accomplish this task and by no means is mine likely the best way, but it worked for me and I wanted to share with the community.  This probably works for most stubborn-to-quit AV products out there, so feel free to re-use and improve upon these techniques yourself if it helps.  Lastly, I did take it a step further and realized I could shut down Cylance across an enterprise domain remotely since I was already using PsExec to elevate privileges..

[](https://2.bp.blogspot.com/-zunBthdon1Q/W2o-KSmuq8I/AAAAAAAAM1Q/0Aa3v5eeGWYyzIEFjflkWikPqBEtXnT3ACEwYBhgL/s1600/PSExec%2BRemote%2BMachine%2BDisable%2BCylance%2BService.PNG)

**Disable Service and Move Files Remotely as SYSTEM Across the Entire Domain!**

**.. but that's just mean! 😉 Until next time!**

Thanks to Lewie for Administration Help & Screen Shots

Thanks to Travis for Being THE MAN

Thanks to my Awesome Team @ [**Pondurance**](https://www.pondurance.com/)!!