STETSON
cybergroup

360 Motor Parkway, Ste 650 | Hauppauge, NY 11788
631.417.3500 | www.stetsoncg.com

SolarWinds Breach and Detection

We have been monitoring all the events going on in the last few days and staying up to date with the news surrounding the breach of SolarWinds. Thanks to the hard work they do at FireEye, they have created the Yara rules to detect the IoC (indications of compromise), that can show if an organization has had the exploits used to create a backdoor to their environment.

We, at Stetson Cybergroup quickly began making a tool to thoroughly test our environment and the clients we support. We created a script that can download the Yara rules created by FireEye and test a computer to see if the back door was created. We feel its our duty to share this tool with the community. You can find the link down below to download and configure this tool for your needs.

What the tool does –

This tool downloads yara64.exe (the scanning engine that uses Yara Rules) from the Virus Total GitHub account and the Yara rules that FireEye made, from our GitHub account. (We will add any IoC's that we come across, so stay tuned for updates!). It then runs the Yara rules across the 4 main locations that the IoC's can be found. Once the scan is done, it checks to see if there were any hits. It then sends an email with any potential hits to an email address you specify. The email contains the attachment telling you what files have been reported as warnings for a possible backdoor. The email is sent using variables from the computer it came from. So, if you are an MSP that has many clients, this will send it out with the computer name and domain as the email address. The goal is to have this run on many computers and report back to the IT Department or MSP Teams. A single bat script that can be run on many machines remotely and report back.

What the tool needs from you –

You will need to set a few options for your organization. You need to tell it how to send out the email and who to send it too. Below is a snippet you will find in the bat file and the changes that are needed. To edit the script, right click the bat file once you download it and click edit. Once you make the changes, you can save (and rename it as needed). Then you just need to run it as admin on any computer you would like to test for the exploit.

Sample taken from bat script (found after the Exit)

```
exit

:: this is where you configure your mail server to send out the email

:::::::$Username = "USERNAME"

:::::::$Password = "PASSWORD"

:::::::$SMTPServer = "MAIL SERVER"

:::::::$SMTPPort = "PORT"

:::::::$To = "EMAIL ADDRESS TO SEND ALERTS TO"

:::::::$SecurePassword = $Password | ConvertTo-SecureString -AsPlainText -Force

:::::::$Credentials = New-Object System.Management.Automation.PSCredential -ArgumentList $Username, $SecurePassword

:::::::$From = "$env:computername" + "@$env:userdomain.com"

:::::::$Attachment = "c:\SolarWindsIOC-$env:computername\Warnings.txt"

:::::::$Subject = "SolarWinds IOC Scan Log from $env:computername"

:::::::$Body = "This is an Automated PowerShell script that creates this data and sends it"

:::::::Send-MailMessage -Attachment $Attachment -From $From -to $To -Subject $Subject -Body $Body -SmtpServer $SMTPServer -port $SMTPPort -UseSsl -Credential $Credentials
```

You will need to set the Username and password to the mail server you're sending this from here.

The mail server your using and the ports to connect to it here. Below that the email address you want the alerts to be sent to.

The rest of this sets the variables needed to send it with context. The final line sends the email out with all of the variables and your settings applied to it.

There you go! After your done configuring those settings save this as a .bat file and you can run it (as admin) on any computer you want to test for the exploits.

What this script cannot do –

Unfortunately, this script is meant for Windows 10+ and Server2012+. It will not run on older OS's.

If you have any issues or concerns running this on your network, feel free to reach out to us. And make sure you stay tuned for updates.

Thanks and stay safe!!

Link to download the script

SolarWindsIOCScanner/SolarWindsIOC-CONFIG MAILER.bat at main · JoeW-SCG/SolarWindsIOCScanner (github.com)