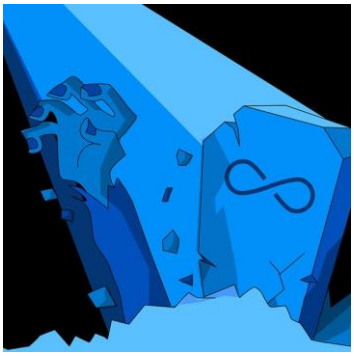

Is EternalBlue Truly Eternal?

Dec 11, 2018

By Omri Inbar, PCYSYS

I build penetration testing software for a living. That means, businesses give our software a *007 license to hack* and our software does a terrific job at it. This is how we validate corporate cybersecurity defenses in an automated manner.In other words, we make an affordable "red-team-in-a-box" software that is extremely fast at penetration testing and is constantly evolving its library of hacking techniques.

Today, penetration testing is commonly performed as an expensive manual service. It is so expensive that it is used to discover a company's vulnerabilities, but never to validate that the necessary remediation indeed took place. This is where everything starts to crumble.

Do you ever wonder how long it takes the IT world to root out malicious malware? The notorious exploit *EternalBlue* (also known as one of the exploits abusing the MS17-010 vulnerability) allegedly used by the NSA and leaked in 2017 was patched by Microsoft. One would assume that 18 months after the fact there would be no remnants of this vulnerability, but I wanted to check myself. I took a break from our company's heavy lifting and spent a night at home building a mobile app to investigate. You would be amazed by how many times I found hosts vulnerable to *MS17-010* still alive and kicking. The exploit allows for a complete takeover of a Windows server that has not been updated since the leak was patched.

How does my app work?

When you open the app, press "Scan" to search for computers in the network (in this case WiFi) which are vulnerable to MS17-010. A scan is initiated and when it's completed, you get a list of susceptible computers, listed by IP. Next, the app delivers the payload using exploits from https://github.com/worawit/MS17-010 compiled to Android with buildozer.

Ordering a change is not equivalent to seeing it through

When given permission, I try the application and can say that one out of five companies has at least one machine with this vulnerability ready to be exploited. It's just unbelievable! Although 2017 is way behind us and millions of customer records have been stolen on account of this vulnerability, the epidemic of MS17-010 has yet to be exterminated. You can often find computers which are still vulnerable, even in enterprises who believe they have patched all of their systems. This can happen despite the best intentions, due to wrongful implementation (human error) of the patch, unwillingness to restart the server patched, or because of compatibility issues with older operating systems. It is critical to understand that even one susceptible computer in a company can be a segway to compromising the entire organization.

In other words, taking over one computer can help a hacker gain foothold in the network and propel his attack forward. My application is a simple application with one attack vector, executed manually, and used to test a network for one specific vulnerability. Think what can be done with a machine which automatically tests for hundreds of vulnerabilities and the interactions between them. My conclusion - one might choose to leave the door open in a bad neighborhood and expect not to be robbed, but that is highly unlikely. I suggest treating your patching the same way: take your patching seriously and validate your fixes with continuous penetration testing software.