BlueKeep

CVE-2019-0708

The vulnerability in Windows OS that has the potential to wreak havoc in organizations.

By:
Eido Epstein

Nov
2019

www.linkedin.com/in/
eido-epstein

INTRODUCTION

The information brought to you in this report was assembled following to the vulnerability being declared by Microsoft on May 14th 2019 and due to the potential impact, it still may have on organizations these days.

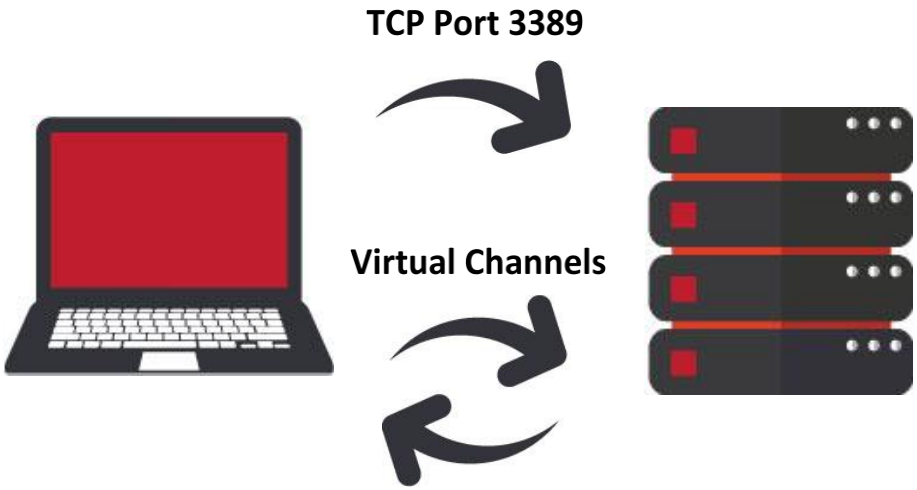
CVE-2019-0708 also known as BlueKeep is a remote code execution vulnerability. Meaning, it can enable hackers to access someone else's computing device and executing malicious codes regardless of the device's geographic location. In order to exploit this vulnerability, the attacker would need to send a special made code request to the target system's Remote Desktop Service via Remote Desktop Protocol.

Following are BlueKeep exploit's main threat capabilities:

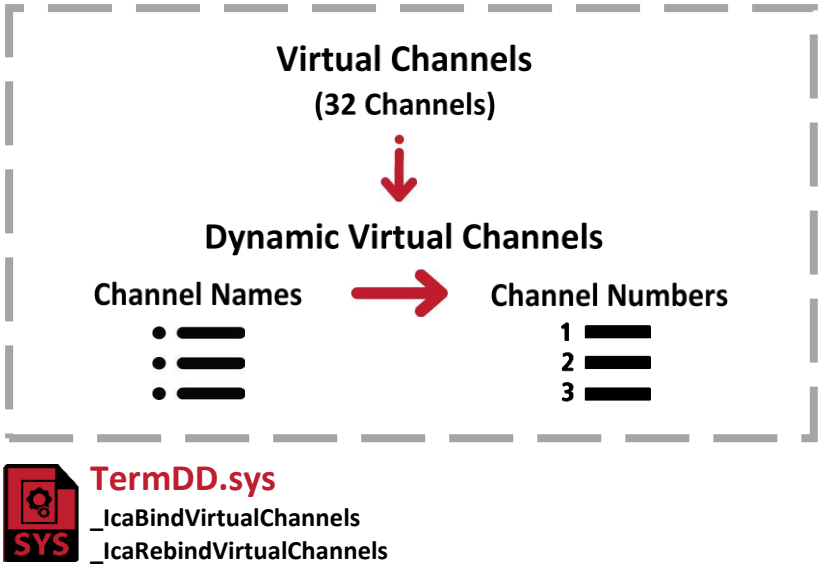
- Viewing, changing or deleting data.
- Creating new system users with full admin capabilities.
- Installing malicious programs like Ransomware and Trojan malware.
- BlueKeep can be warmable, meaning, it can spread to other devices with the same vulnerability.

HOW IT WORKS

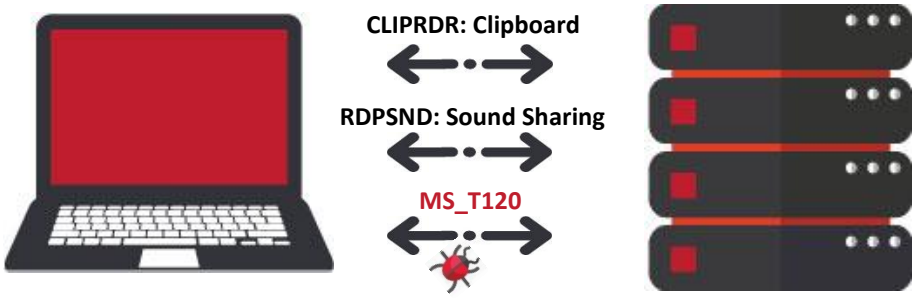
In order for RDP to enable users to connect remotely to a Windows session, a default connection occurs with TCP Port 3389 between the computer and server. Enabling them to transfer data via Virtual Channels.



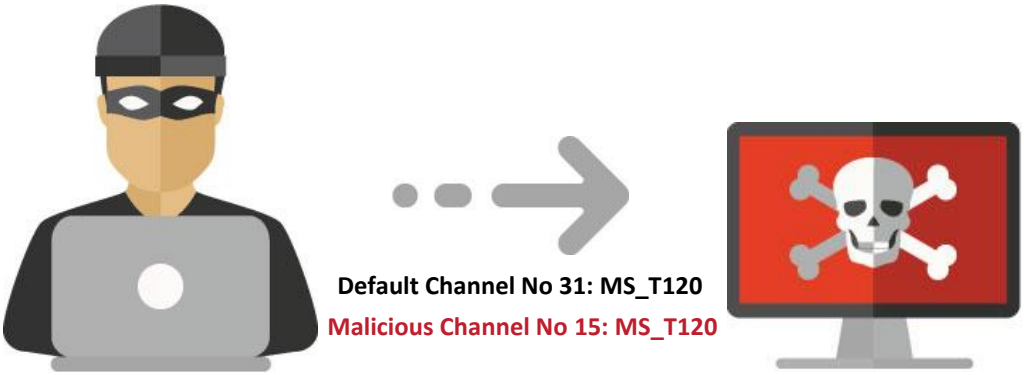
Virtual Channels are usually set to a default number of channels. In Window XP and Server 2003 that number is thirty-two. In order to bypass this limitation Dynamic Virtual Channels were created. Windows binds the Virtual Channel Names to Channel Numbers within the driver TermDD.sys. And to be more specific, within the functions _IcaBindVirtualChannels and _IcaRebindVirtualChannels



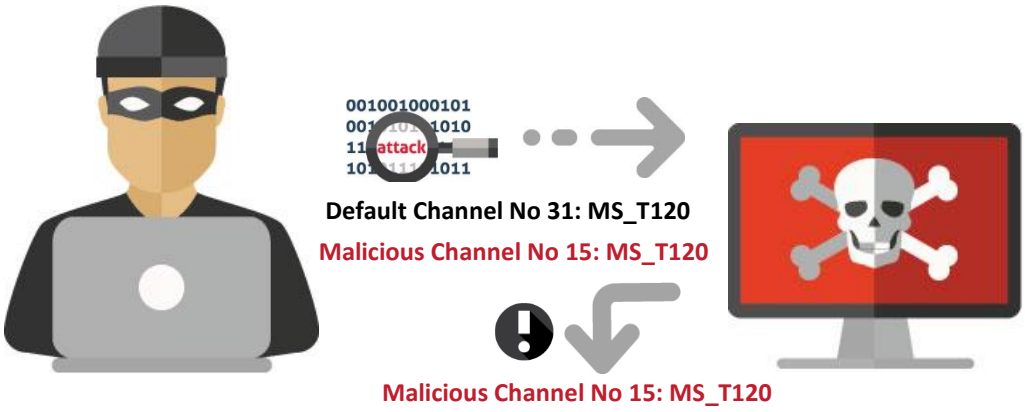
Channels are referenced in Windows with different names and can be used for different purposes.
By default, RDP reserves channel thirty-one with the name MS_T120 but does not check the existence of two channels with the same name. This is where the vulnerability lies.



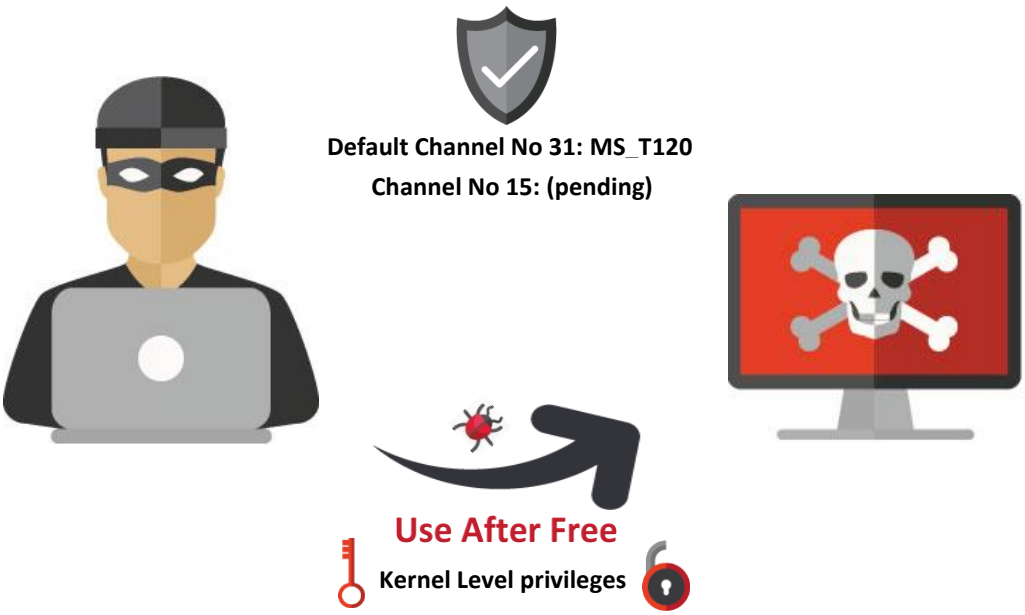
An attacker can set-up this name with a different channel number. Resulting in the current RDP session to have the same MS_T120 in two different places within the thirty-two channels available.



When the attacker sends crafted data through the malicious channel the driver TermDD.sys will attempt to close the channel and terminate the RDP session.



With the malicious channel closed, the referenced pointer will be clear for channel fifteen. But a dangling pointer will remain, tied to channel thirty-one. Leading to a Use After Free vulnerability, that enables the attacker to predict space in memory, to write arbitrary code and execute malicious payloads. In this case with Kernel Level privileges.



AVAILABILITY

In its early months since it was declared by Microsoft. Many researchers and organizations were referring from publicly publishing any Proof of Concept for BlueKeep "into the wild", concerning the abusive use hackers will have with them. As of Nov 1th 2019, the day this report was written. POC versions of BlueKeep that can be altered in order to take part in fraudulent activity are starting to be published. Although this POCs are not fully functional for malicious activity, many data these days about modifying them to be an active BlueKeep exploit is being available publicly. It is also important to mention that already-build BlueKeep exploit codes are also beginning to surface;

Figure 1: One of many BlueKeep POC versions available to be download from GitHub. That can be modified for malicious activities.

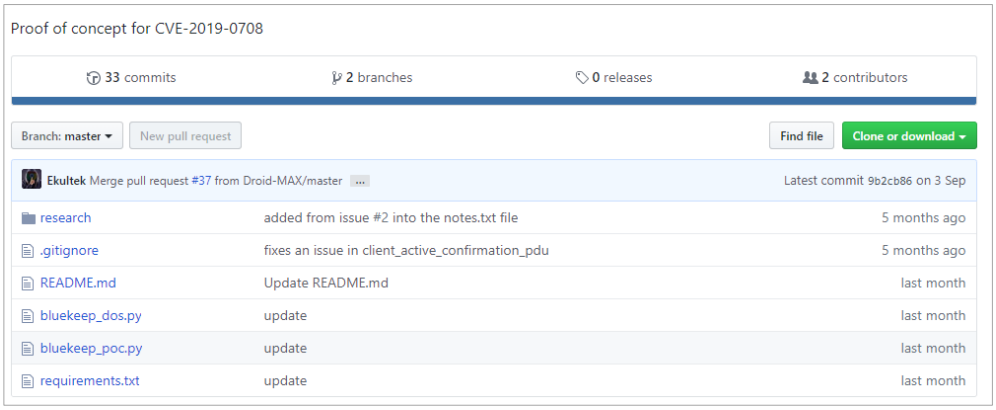


Figure 2: A BlueKeep exploit repository available on GitHub for Metasploit- an open source penetration testing software used by penetration testers and hackers.

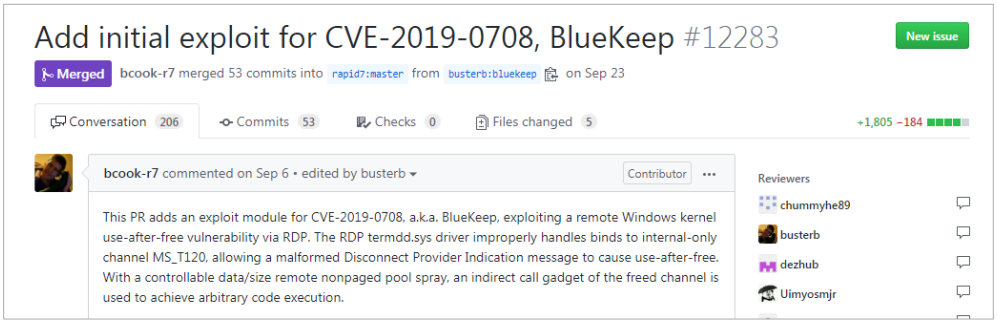
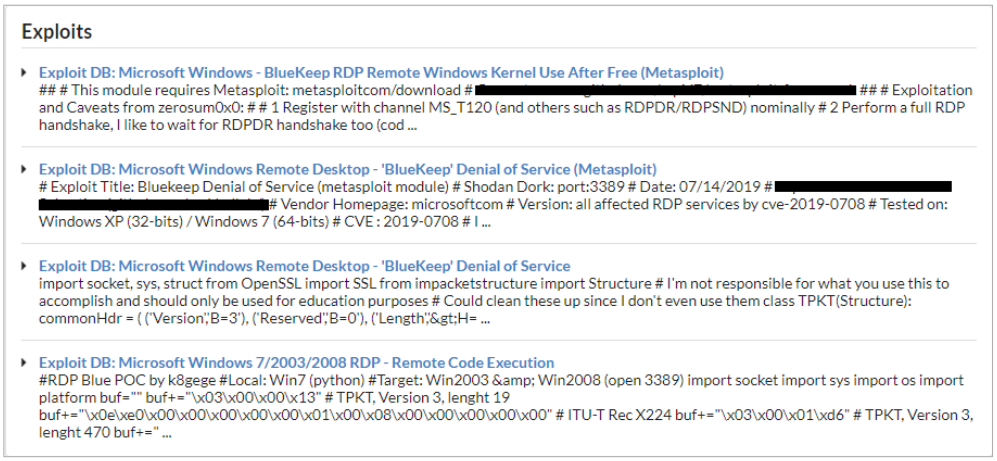


Figure 3: A gathered collection of BlueKeep exploits available "in the wild". Some of the codes are easier to be modified for malicious activities then others.



THE THREAT

As previously mentioned, attackers exploit BlueKeep via RDP. In order to gain access to the organization's operating systems, port 3389 which handles RDP is needed to be open in order to enable the attacker to remote access to the targeted network.

Even today, although we are aware of this vulnerability since May 14th. There are approximately five million computing devices that port 3389 is open for them and they are able to receive Remote Desktop Service requests from other entities outside of their network.

Hackers are aware of the wide magnitude of potential victims and the wide range of abusive capabilities they can have with the exploit. And they are eager to use it;

Figure 4: The hackers in this forum try to understand how to activate the POC in Figure 1 as an exploit.

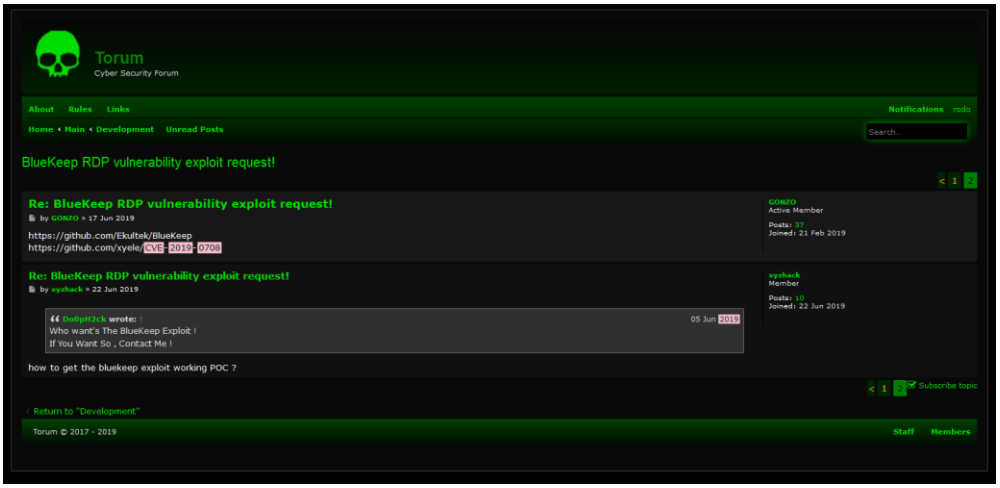
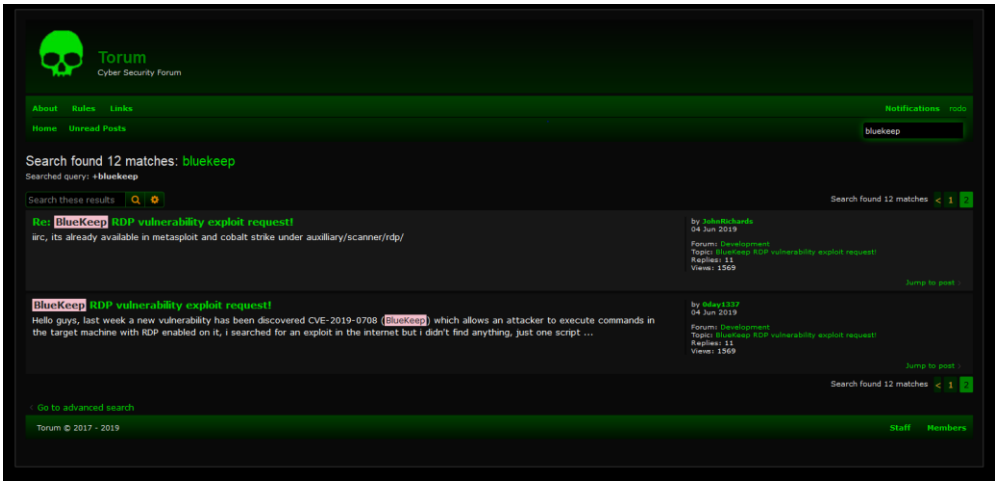


Figure 5: In the same forum, hackers are discussing that an exploit is being available in Metasploit.



The potential risk to organizations does not end with the availability of computing machines with an open 3389 port. Many companies these days are referring to cloud hosting services for testing their applications or hosting their private data. One well known company that provides such services is AWS- Amazon Web Services, that not only provides custom build hosting options but also enables the user to choose is Operating System. Many companies, much like AWS are providing their services with

Microsoft's operating systems which were found to be compromised for a BlueKeep exploit.

Following are Microsoft's operating systems that may pose as a risk for a BlueKeep exploit:

System Name	Info
Windows 7 (x32) (x64)	Vulnerability detected on OS.
Windows Server 2008 (x32) (x64) (Itanium)	Vulnerability detected on OS.
Windows Server 2008 R2 (x64) (Itanium)	Vulnerability detected on OS.
Windows XP (x32) (x64)	No longer supported by Microsoft.
Windows Server 2003 (x32) (x64) (Itanium)	No longer supported by Microsoft.
Windows Vista (x64)	No longer supported by Microsoft.

One of AWS services; DaaS- Desktop as a Service, provides in its features a Windows 7 OS. A system that was previously investigated by Microsoft and found to have a BlueKeep vulnerability. Just to understand the potential risk at hand, AWS claims to have hundreds of thousands managed desktops in her DaaS service.

In addition to that, another service of AWS, EC2- Elastic Compute Cloud can support Windows Servers 2003 and 2008. These systems may also pose as a risk for a BlueKeep exploit. Although the number of EC2 clients was never disclosed, their customers can vary from personal users to start-ups, organizations and financial institutes.

Because BlueKeep is warmable, cloud hosting services not only pose as a risk, they can also prove to be as a source of infection to the entity who use them. Enabling the exploit to search for more vulnerable operating systems by using the cloud hosting infrastructure that's connected to the relevant entity.

MONITORING

After we reviewed the potential risk BlueKeep pose to organizations. It's time to present the tools we can use to detect it. In order to make sure that your computing devices will not be compromised.

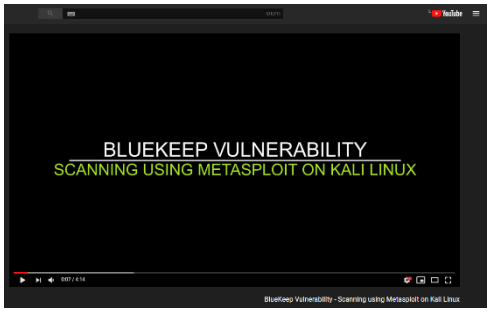
All of the tools that enable organizations to detect a BlueKeep vulnerability focus on monitoring RDP communication in general and some are more specific and focus on inspecting the MS_T120 channel.

It is important to note, that if your organization is using a third party's security or cloud services. It is advised to consult with them and verify whether or not they have updated their malicious detection policies for BlueKeep. For this report we'll note two of the free of charge possibilities available;

1. **RDPScan by Robert Graham.**
   Security researcher Rob Graham created an RDP scanner for detecting BlueKeep vulnerability.

2. **Metasploit (**MSF: AUXILIARY/SCANNER/RDP/CVE_2019_0708_BLUEKEEP**).**
   A penetration testing software used by penetration testers and hackers alike. Its community module builders created a scanner for BlueKeep vulnerability.

Figure 5: A short video on YouTube explaining how to scan for a BlueKeep vulnerability with the relevant module (MSF) in Metasploit.



MITIGATION

The steps you need to take in order to make sure the information in your organization is properly protected from this exploit;

1. **Patch Your Systems (**Link1**,** Link2**).**
   As the vulnerability was detected, Microsoft released a patch for all of the systems that were detected with it, as well as systems that do not receive mainstream support any longer. It is highly advised by Microsoft to patch these systems as the potential severity of this vulnerability is considered as critical.

2. **Block/Restrict Port 3389.**
   As was previously mentioned in this report. One of the methods hackers have is to scan the internet for an open 3389 port for using this exploit. In order to prevent such attempts, it is advised to block/restrict port 3389 in your network.

3. **IP Address Restriction.**
   Use firewalls to restrict Remote Desktop access so that only a specific IP address can have access to a particular device.

4. **Establish NLA- Network Level Authentication in Your Enterprise.**
   By configuring this option on your organization's servers, you are creating another security layer. NLA completes a user authentication process before establishing any remote desktop connection. Making it harder for hackers to exploit any remote code execution vulnerabilities that your systems may have.

CONCLUSION

Although this vulnerability was initially published on May 14th 2019, there are still major concerns in the cyber intelligence and security fields regarding the potential harm BlueKeep may cause. The extensive scope of users and organizations that can be compromised and the will of hackers to always improve and find new ways to use an exploit, is what keeps these communities restless. And although some counter measures were already revised, some companies still haven't yet properly protected themselves.

I will make the efforts to update this report with any new knowledge published for the vulnerability or exploit, In order to make sure that any entity who reads this report keeps itself the most knowledgeable they can be regarding this matter.

Mail: eidoepstein@gmail.com
Phone: (+972) 507-513-270
LinkedIn: www.linkedin.com/in/eido-epstein