

关于 基于 SMB 文件共享传  
击  
全 告



360安全监测与响应中心

2017 05 12

<b>第 1 章 安全通告</b> .....	<b>3</b>
<b>第 2 章 漏洞信息</b> .....	<b>4</b>
2.1 .....	4
2.2 .....	4
<b>第 3 章 处置建议</b> .....	<b>5</b>
3.1 .....	5
3.2 .....	5
.....	5
.....	5
.....	7
3.3 .....	7
3.4 .....	7
<b>第 4 章 技术分析</b> .....	<b>8</b>
4.1 体    估 .....	8
4.2 .....	8

# 第1章

：

2017 5 12 ， 中 于 Windows 享  
传 代 ， 不 之 NSA  
中 “ 之 ” 事件。

会 445 件 享 Windows ， 任  
何 作， 上 ， 不 中 、  
、 。

445 严 企业 传  
， ， 会 ， 不 付  
会 严 。 事件 严 ，  
企业 也 临 。

360 与 中 也 事件 ， 一 为  
事件信 。

： 京 2017 4 14 ， 一 NSA  
Shadow Brokers ， 中 了 个 Windows  
(SMB、RDP、IIS) 令 。

## 第2章 信

### 2.1

企业 WannaCry 事件，  
件会，付件，严。  
，不 NSA “之  
”传事件。代会 445 件享  
Windows，任何作，上，不  
中件、。  
于以 445 传，主上  
了 445，但企业且  
丁，仍 445 且，。

### 2.2

360 与 中 事件 为：

## 第3章

### 3.1

， 445 SMB ， 于 Win7  
以上 了 MS07-010 丁， 。Win7  
以下 Windows XP/2003 丁， SMB 。

### 3.2

传 ， 360 企业  
上 445 ， 上 IPS 360  
之 ，  
， 了 MS07-010 丁 了 Server 。

Server 。

Server :

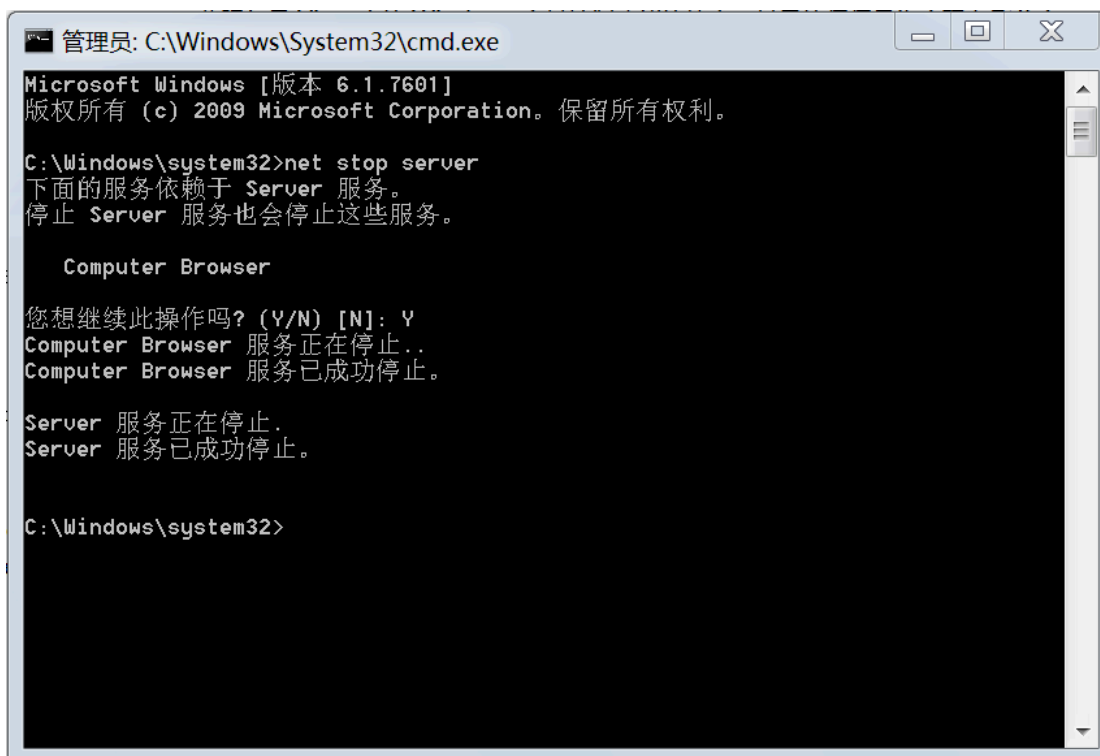
- 1、 ， ， cmd，
- 2、 令: netstat -an
- 3、 中 445

```
C:\Windows\system32>netstat -an

活动连接

 协议 本地地址          外部地址          状态
TCP    0.0.0.0:135        0.0.0.0:0         LISTENING
TCP    0.0.0.0:443        0.0.0.0:0         LISTENING
TCP    0.0.0.0:445        0.0.0.0:0         LISTENING
TCP    0.0.0.0:902        0.0.0.0:0         LISTENING
TCP    0.0.0.0:912        0.0.0.0:0         LISTENING
TCP    0.0.0.0:1025       0.0.0.0:0         LISTENING
TCP    0.0.0.0:1026       0.0.0.0:0         LISTENING
TCP    0.0.0.0:1027       0.0.0.0:0         LISTENING
TCP    0.0.0.0:1031       0.0.0.0:0         LISTENING
TCP    0.0.0.0:1032       0.0.0.0:0         LISTENING
TCP    0.0.0.0:1046       0.0.0.0:0         LISTENING
TCP    0.0.0.0:3389       0.0.0.0:0         LISTENING
TCP    0.0.0.0:15000      0.0.0.0:0         LISTENING
TCP    0.0.0.0:54321      0.0.0.0:0         LISTENING
TCP    127.0.0.1:443      127.0.0.1:3605    ESTABLISHED
TCP    127.0.0.1:443      127.0.0.1:3607    ESTABLISHED
TCP    127.0.0.1:443      127.0.0.1:3613    ESTABLISHED
TCP    127.0.0.1:443      127.0.0.1:3614    ESTABLISHED
```

445，Server，以 Win7 为例，作  
下：  
，中 cmd，上 cmd  
，以份，cmd 中 “net stop server” 令，  
会下：



```
管理员: C:\Windows\System32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>net stop server
下面的服务依赖于 Server 服务。
停止 Server 服务也会停止这些服务。

    Computer Browser

您想继续此操作吗? (Y/N) [N]: Y
Computer Browser 服务正在停止..
Computer Browser 服务已成功停止。

Server 服务正在停止.
Server 服务已成功停止。

C:\Windows\system32>
```

于 。

### 3.3

于 Win7 以上 作 ， 丁 MS17-010 修 了“  
之 ” ， 丁。 于 于  
， 使 Server ， 作 。

于 Windows XP、2003 不 供 ， 使 360  
“NSA ” ，  
以 侵 。 下 ；  
<http://dl.360safe.com/nsa/nsatool.exe> 。 些 作  
， 。

### 3.4

业 份， 业  
像， 作 。

## 第4章

### 4.1 体 估

事件 445 , 。

### 4.2

企业 事件 。