

## 来自BlackHat的新姿势：Process Doppelgänger攻击技术与贴身防护

360安全卫士 2018-01-12 共54199人围观，发现2个不明物体

系统安全

2017欧洲黑帽大会（Blackhat EUROPE 2017）上，网络安全公司enSilo两名研究人员介绍了一种名为“Process Doppelgänger”的新型攻击。该攻击技术可以针对windows vista以上所有版本平台发起攻击，甚至可绕过大多数现主流安全软件的检查，执行恶意程序。

此攻击技术披露后，360安全卫士主动防御体系进行了紧急升级，对Process Doppelgänger的诸如和进程创建等攻击为进行了多维度拦截，完美破解了攻击的“反侦察”技术，为用户实现了贴身保护。

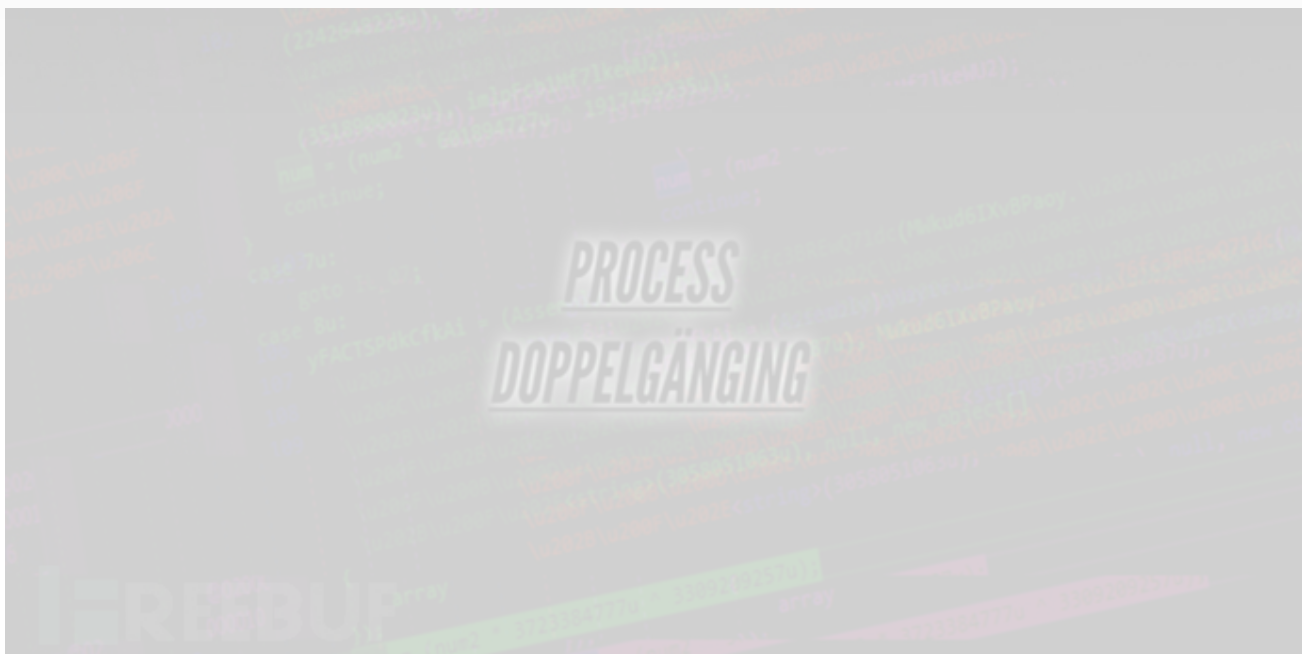


图1

### 0×01攻击原理

微软从Windows Vista开始支持NTFS Transaction（TxF），最初的目的是用于文件升级和分布协同

（Distributed Transaction Coordinator，DTC）等场景，可以回滚修改操作。Process Doppelgänger攻击利用TxF的可以滚的特性，（1）先用恶意程序写覆盖白程序，（2）然后将覆盖后的文件加载到内存，（3）加载完成后回滚磁盘文件为写覆盖之前的文件，（4）最后利用（2）加载到内存中的Section创建进程，最终达到执行恶意程序并绕过杀检查的目的。



首先创建一个事务：



图2

将白程序文件添加到这个事务：

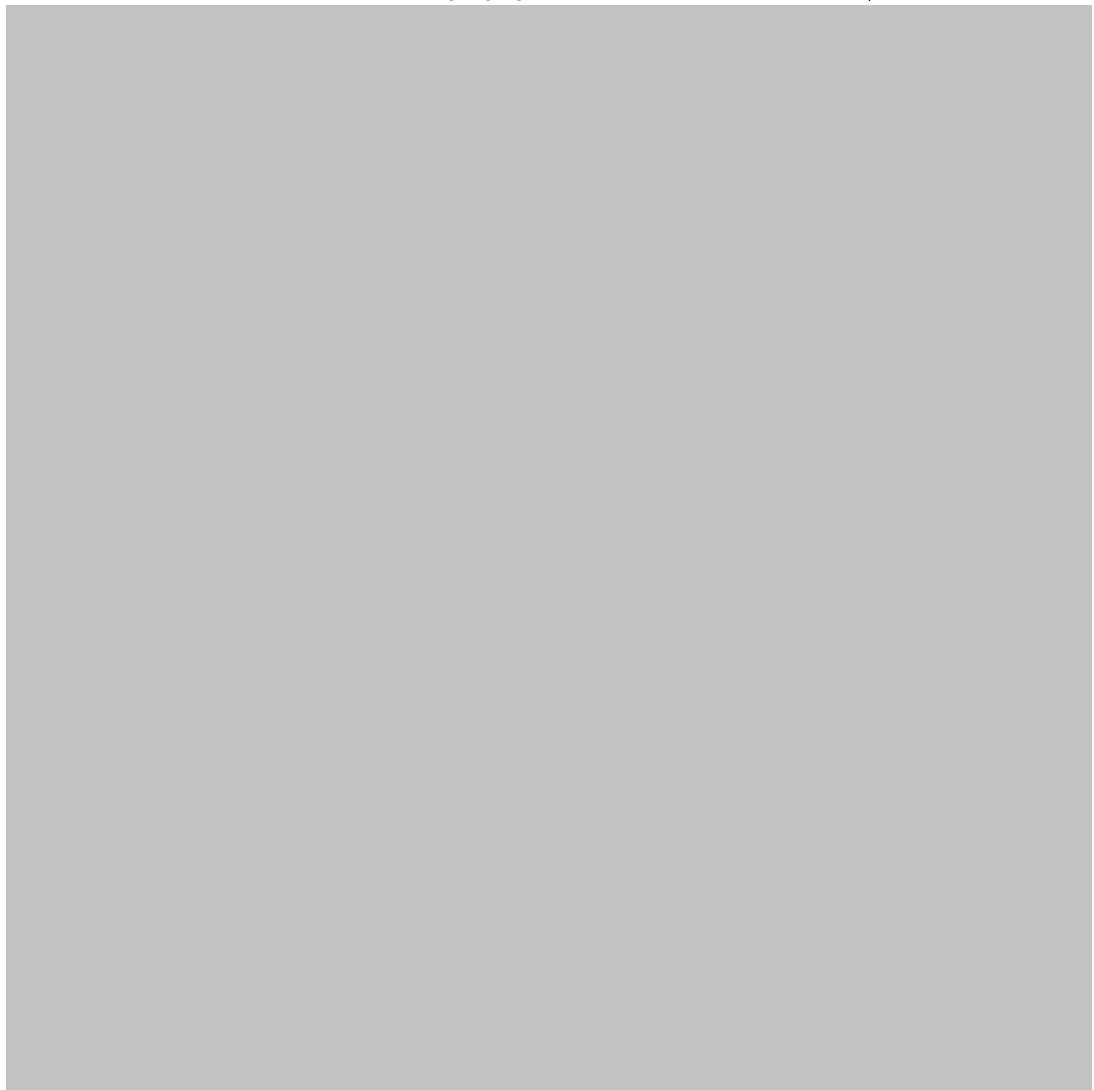


图3

用恶意程序覆盖：

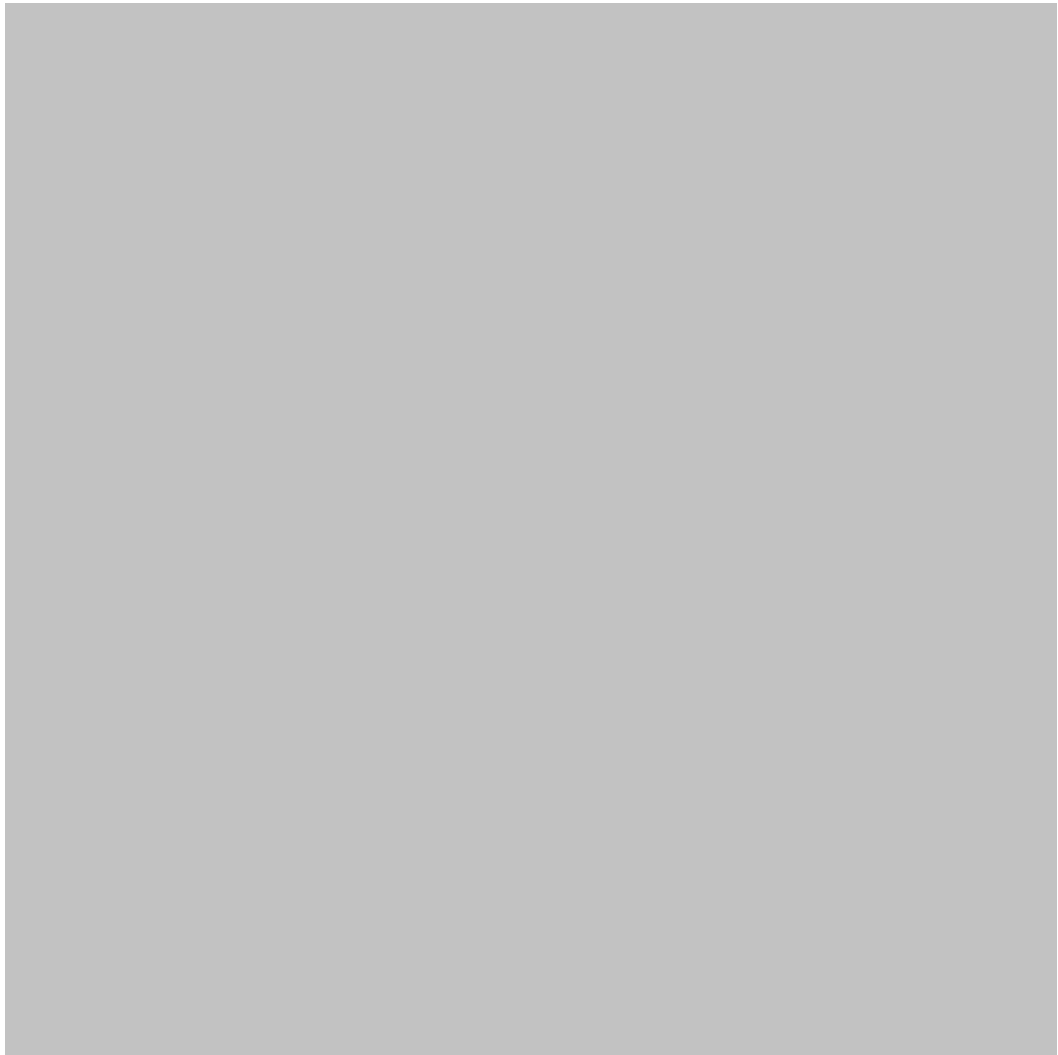


图4

加载到内存：

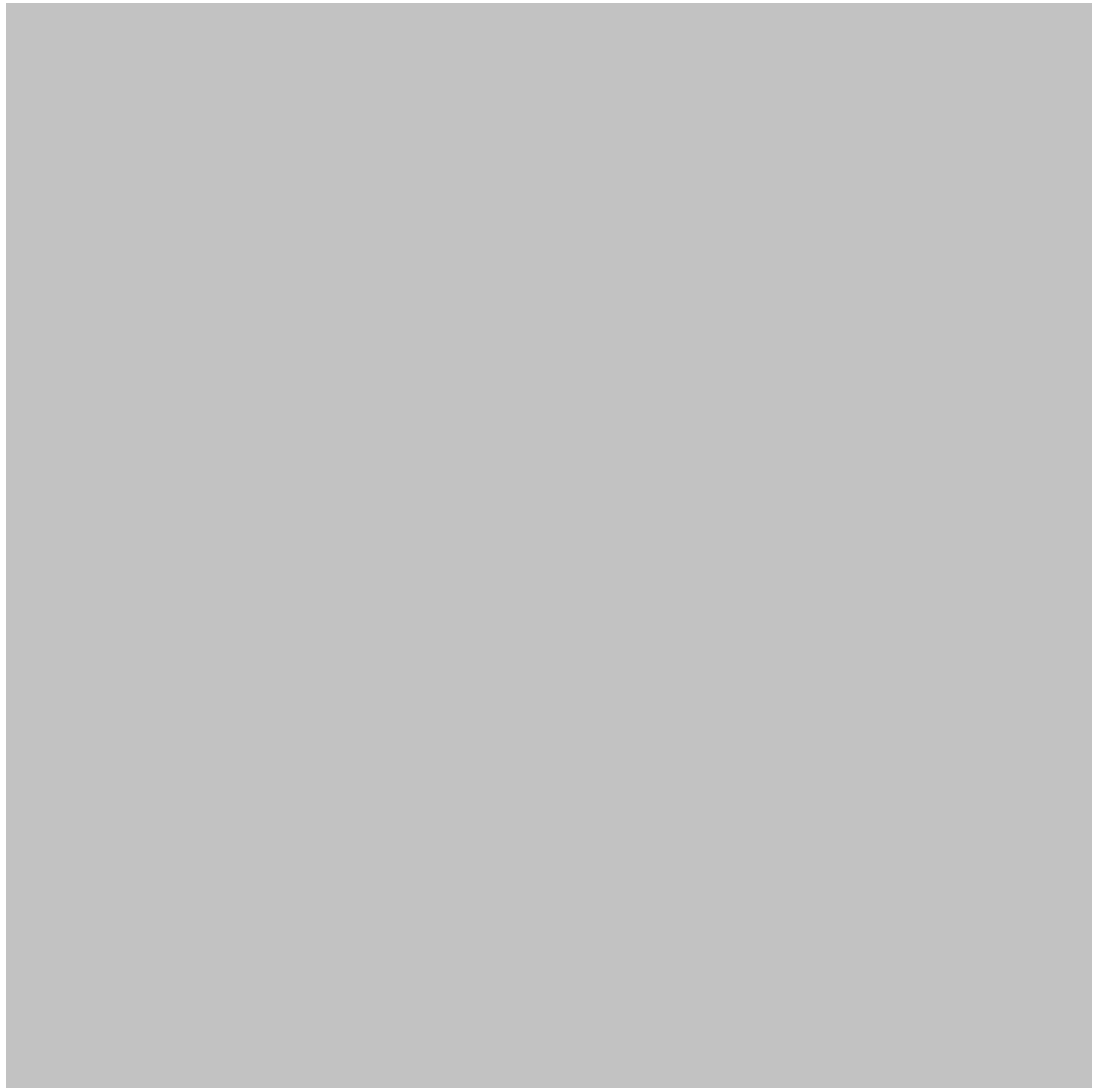


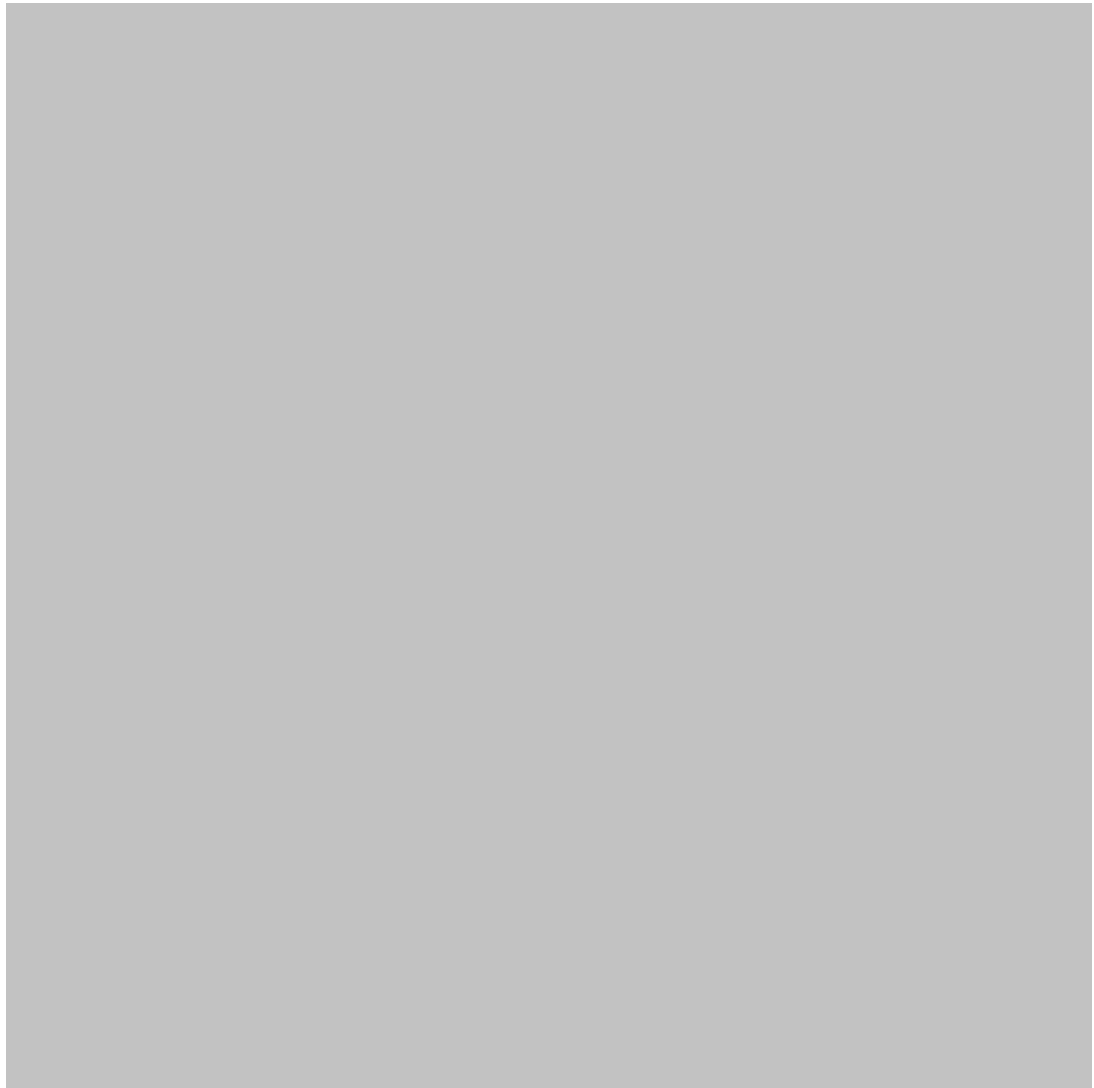
图5

回滚事务：



图6

最后利用内存中的Section创建进程：



### 0×03攻击效果

该攻击方式可以绕过国外主流防护软件。





图8

## 0×04 360安全卫士防御升级

360安全卫士针对此攻击方式，进行了防护强化，增加了多维度的保护，对攻击的注入和进程创建行为均进行拦截，保护用户电脑安全。



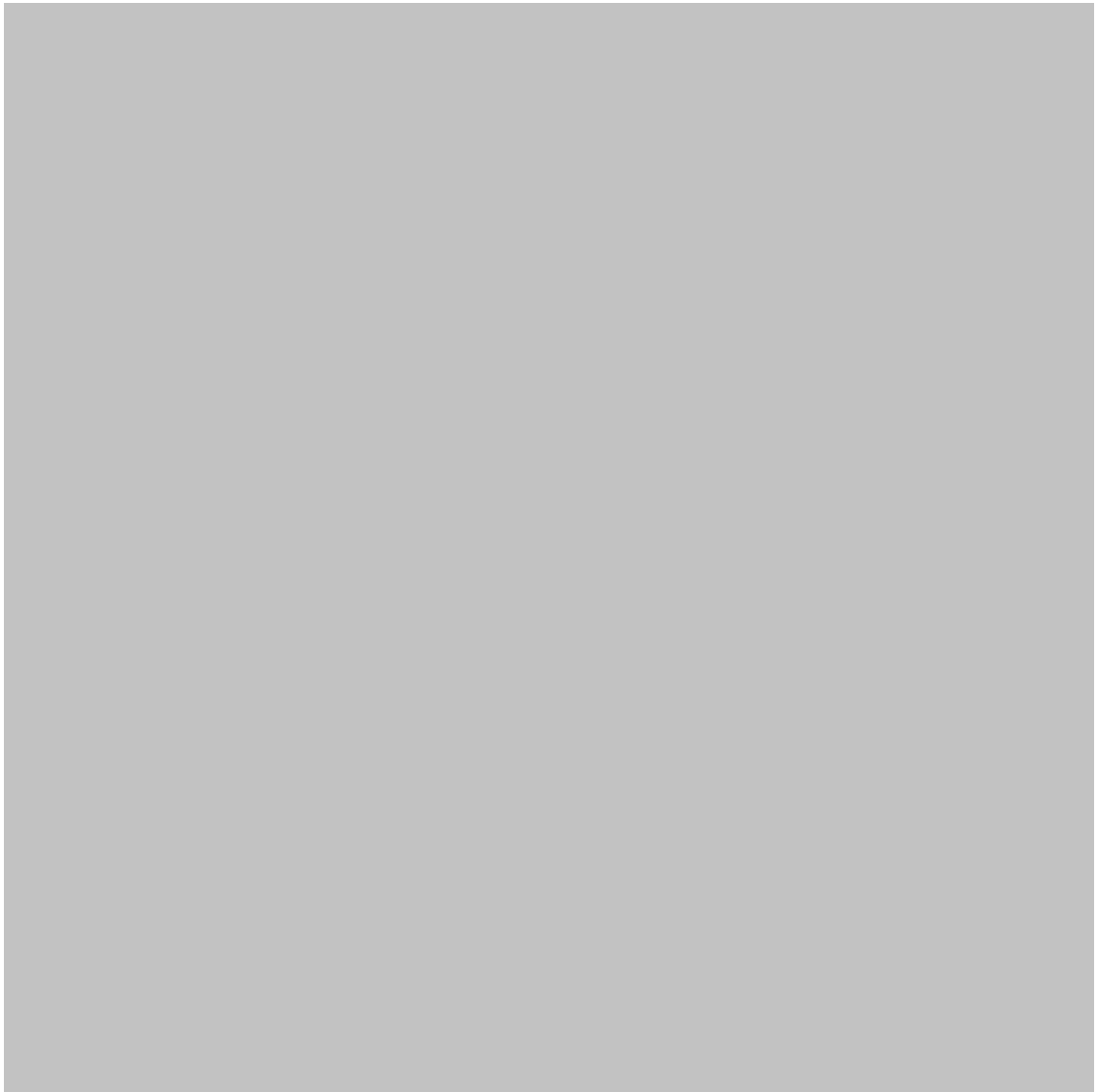


图 9





图10

\*本文作者：360安全卫士，转载请注明来自FreeBuf.COM

上一篇：[Android恶意软件偷取Uber凭证](#)

下一篇：[快讯 | macOS漏洞导致本地管理员可以使用任何密码解锁App Store系统设置](#)

## 已有 2 条评论

幕刃 2018-01-12

1楼 [回](#)

我还以为自己穿越了

[亮了](#)

吴涛 2018-01-12

2楼 [回](#)

选择文件

未选择任何文件

昵称

请输入昵称

必须

您当前尚未登录。[登陆?](#) [注册](#)

邮箱

请输入邮箱地址

必须（保密）

表情

插图

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



[360安全卫士](#)

360安全卫士官方账号

158

文章数

10

评论数

最近文章

- [来自BlackHat的新姿势：Process Doppelganging攻击技术与贴身防护](#)

2018.01.12
- [简要指南 | 处理器Meltdown & Spectre漏洞修复](#)

2018.01.10
- [“噩梦公式”二代 | 2018年微软修复的首个Office 0day漏洞（CVE-2018-0802）分析](#)

2018.01.10

浏览更多

[DEFCON精彩破解：Apple Pay被攻破...](#)[BlackHat议题：利用卫星接收器拓展僵...](#)[\[预告\]Freebuf将推出BlackHat2012专题](#)[传P0sixninja在黑帽大会上出售了越狱...](#)[BlackHat议题：SMB不只是共享你的...](#)

## 特别推荐



[【FB TV】一周「BUF大事件」：  
WPA2惊现高危漏洞，你的WiFi还](#)

[willhuang](#)

2017-10-21

[【已结束】第三届中国\(北京\)军民  
融合技术装备博览会现场实况](#)

[Elaine\\_z](#)

2017-07-03

[技术剖析：海莲花（OceanLotus）  
根本不是APT，它只是一个普通木](#)

[毒舌评论砖家](#)

2015-06-03


[Windows 10新变化：系统自动更新  
将“强制化”，用户不再可选](#)

[dawner](#)

2015-07-20



Copyright   2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务

