2018年Windows漏洞年度盘点

腾讯安全联合实验室 / 2019-01-25 09:36:00 / 浏览数 4874 技术文章 技术文章 顶(0) 踩(0)

一、 前言

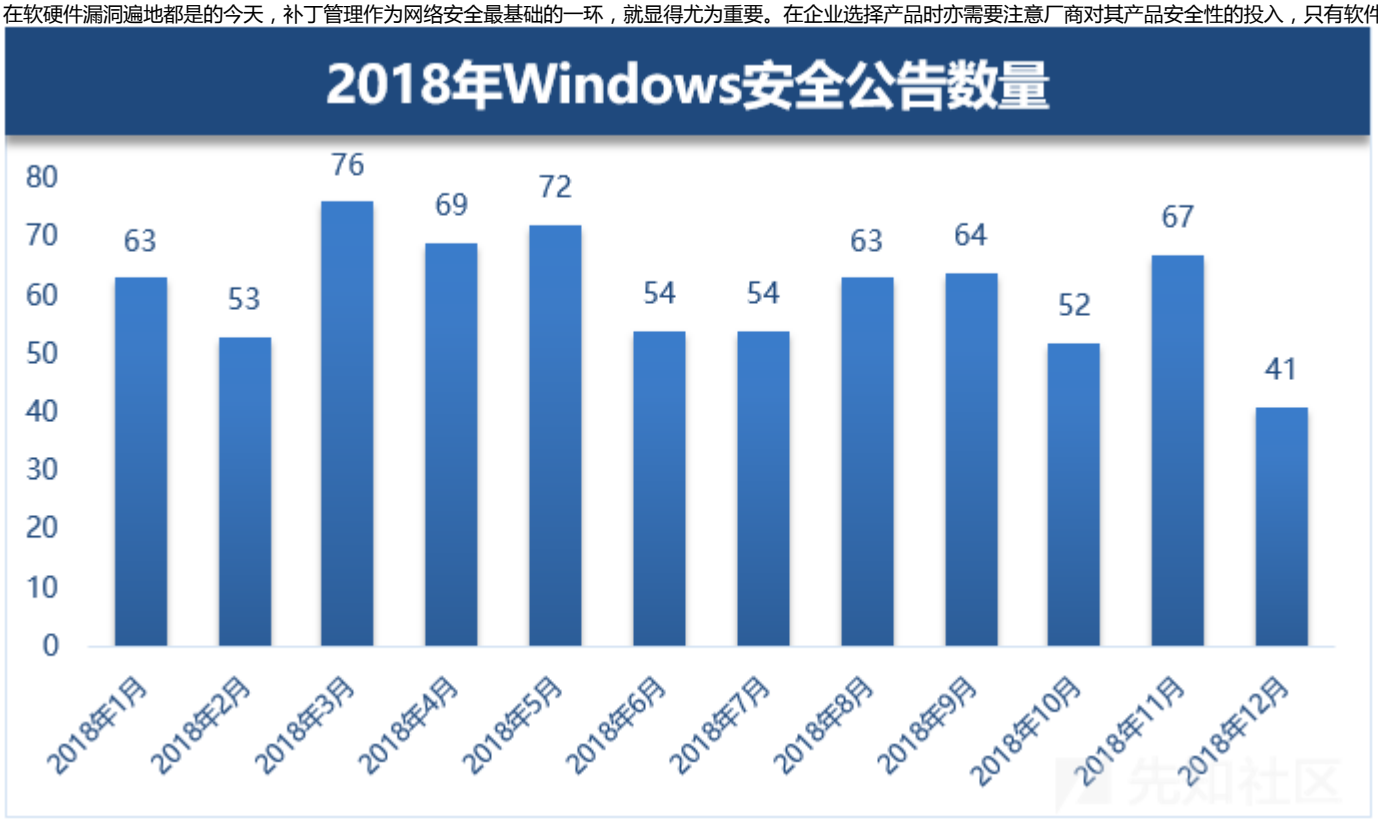
漏洞是影响网络安全的重要因素，而漏洞攻击作为恶意攻击的最常用手段，更是有着目标行业化、手段多样化的趋势，不论是个人还是企业，都面临着严峻的漏洞威胁。
2018年在轰动式的“幽灵”、“熔断”两大CPU漏洞中揭开序幕。“震网3漏洞利用挖矿”、“412挂马风暴”等安全事件发生表明，漏洞利用攻击，不再是APT组织的“专属”，漏洞利

二、 2018年Windows平台漏洞盘点

2018年对于安全行业是颇具考验的一年，据安全数据库网站cvedetails.com的漏洞提交数据统计，自1999年起，Windows操作系统的漏洞提交数量就呈逐年上涨的趋势，

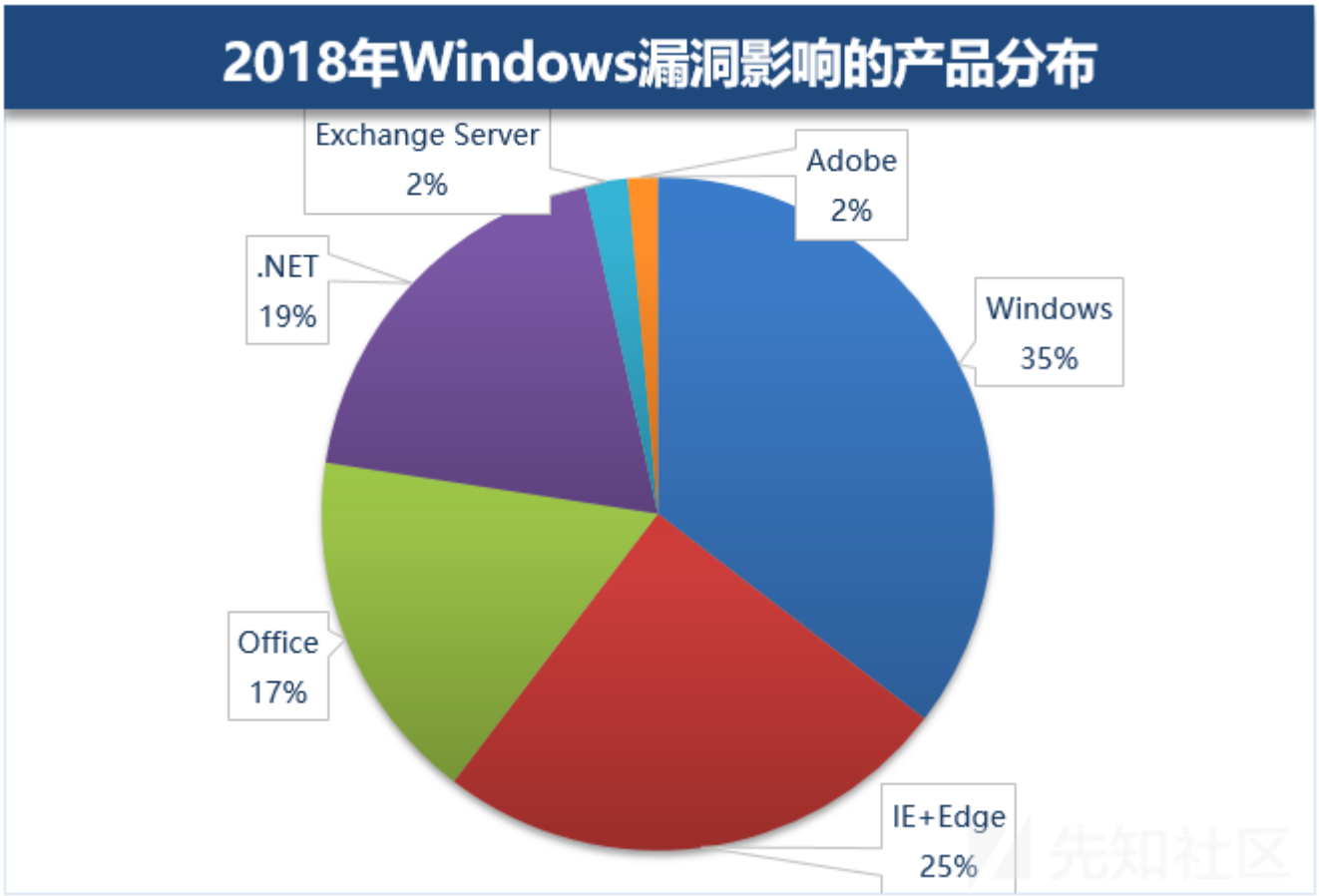
2.1 2018年Windows安全公告数量

在软硬件漏洞遍地都是的今天，补丁管理作为网络安全最基础的一环，就显得尤为重要。在企业选择产品时亦需要注意厂商对其产品安全性的投入，只有软件/平台开发商对

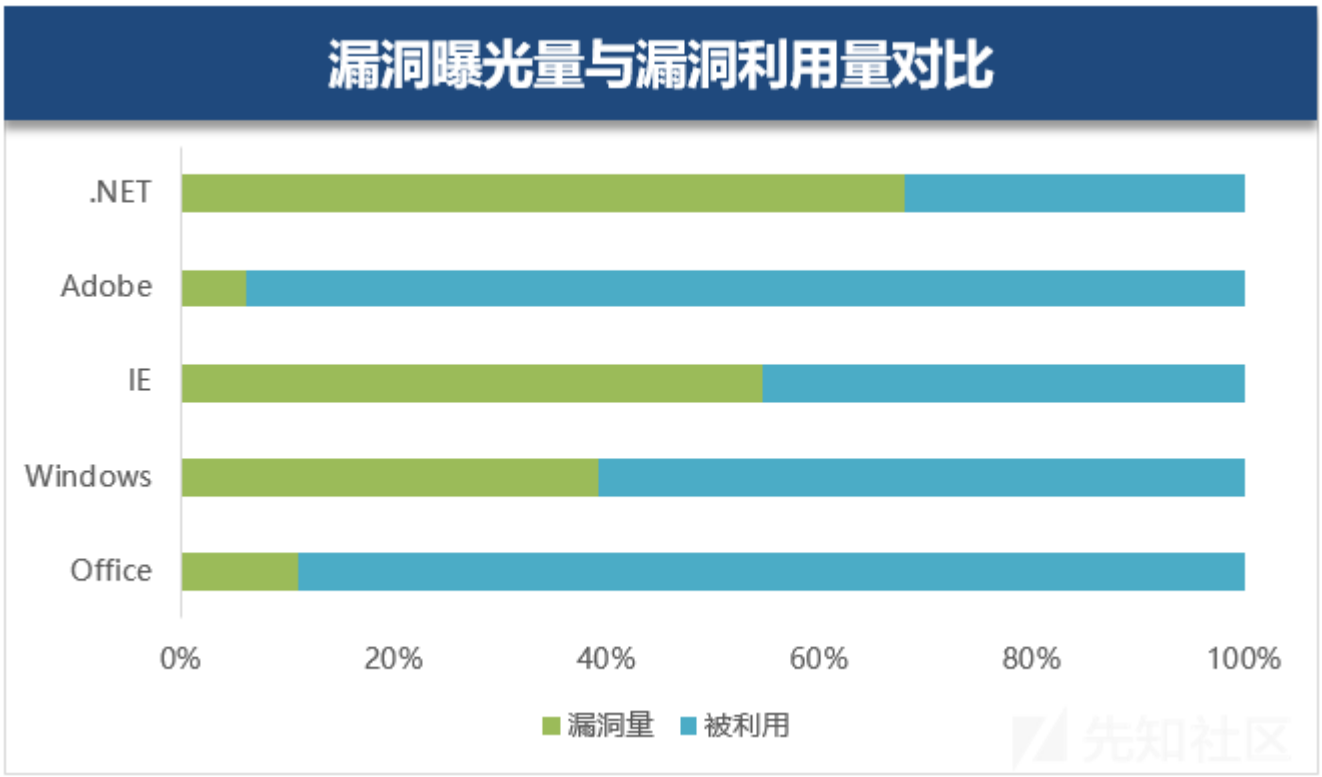


2.2 Windows漏洞影响产品&系统分布

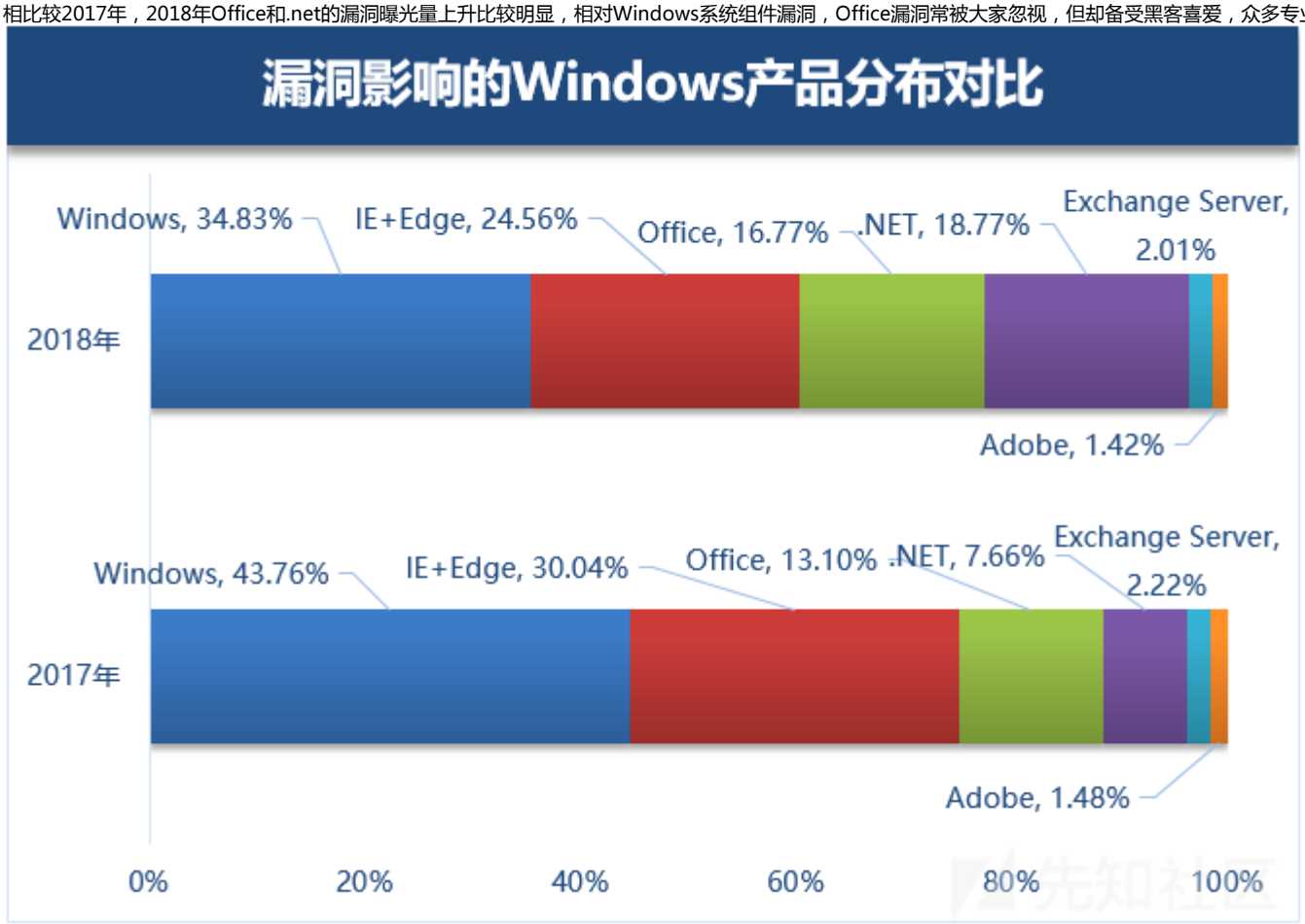
2018年，在所有漏洞影响的Windows产品中，Windows系统组件漏洞占到了35%的比例，浏览器漏洞占25%，Office漏洞则占比17% 。



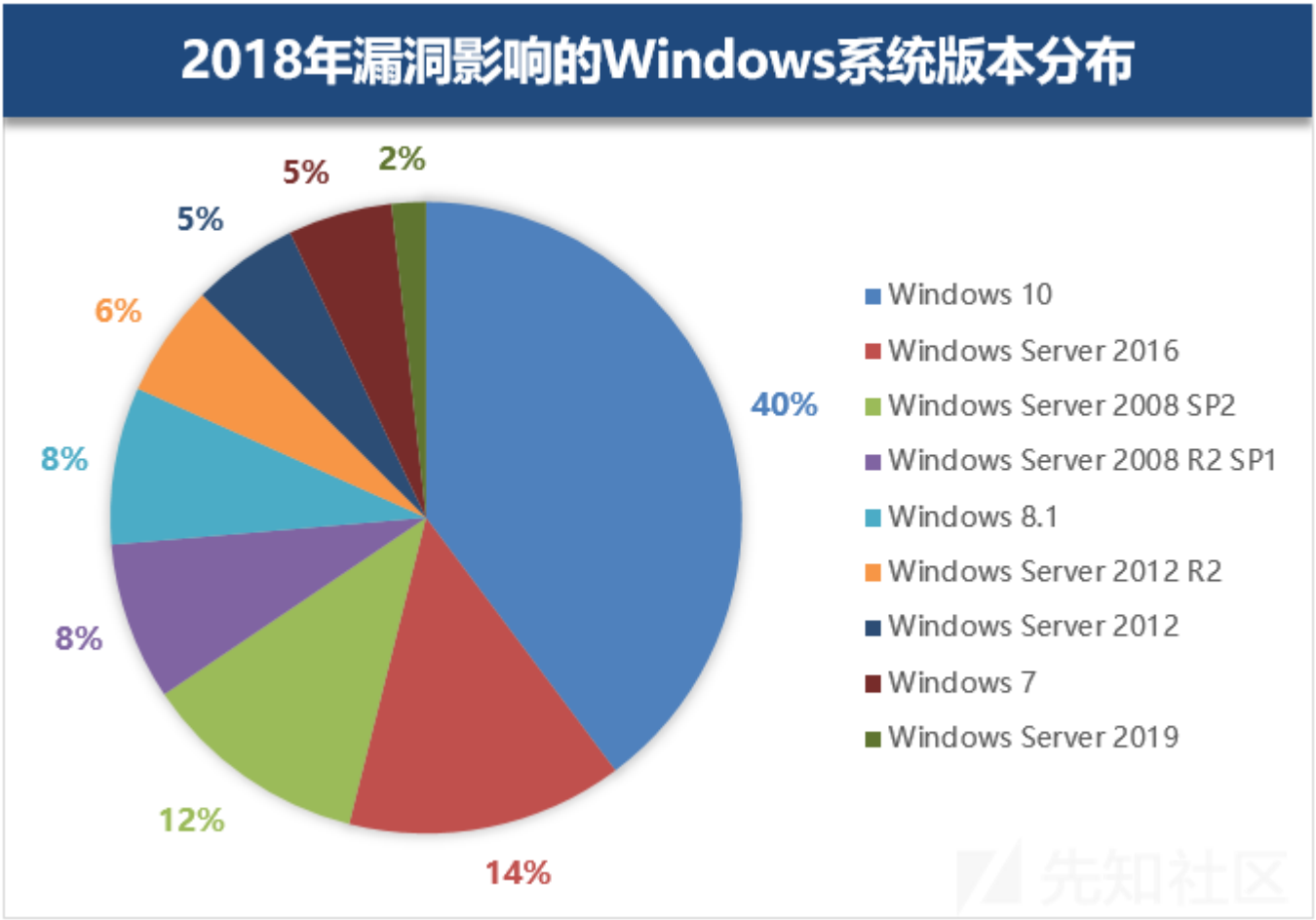
根据腾讯御见威胁情报中心的数据监测，虽然Office和Adobe(主要是Flash)被曝光的漏洞相对较少，但漏洞利用的比例最高。可见，黑客挑选漏洞时，更可能是优先考虑漏



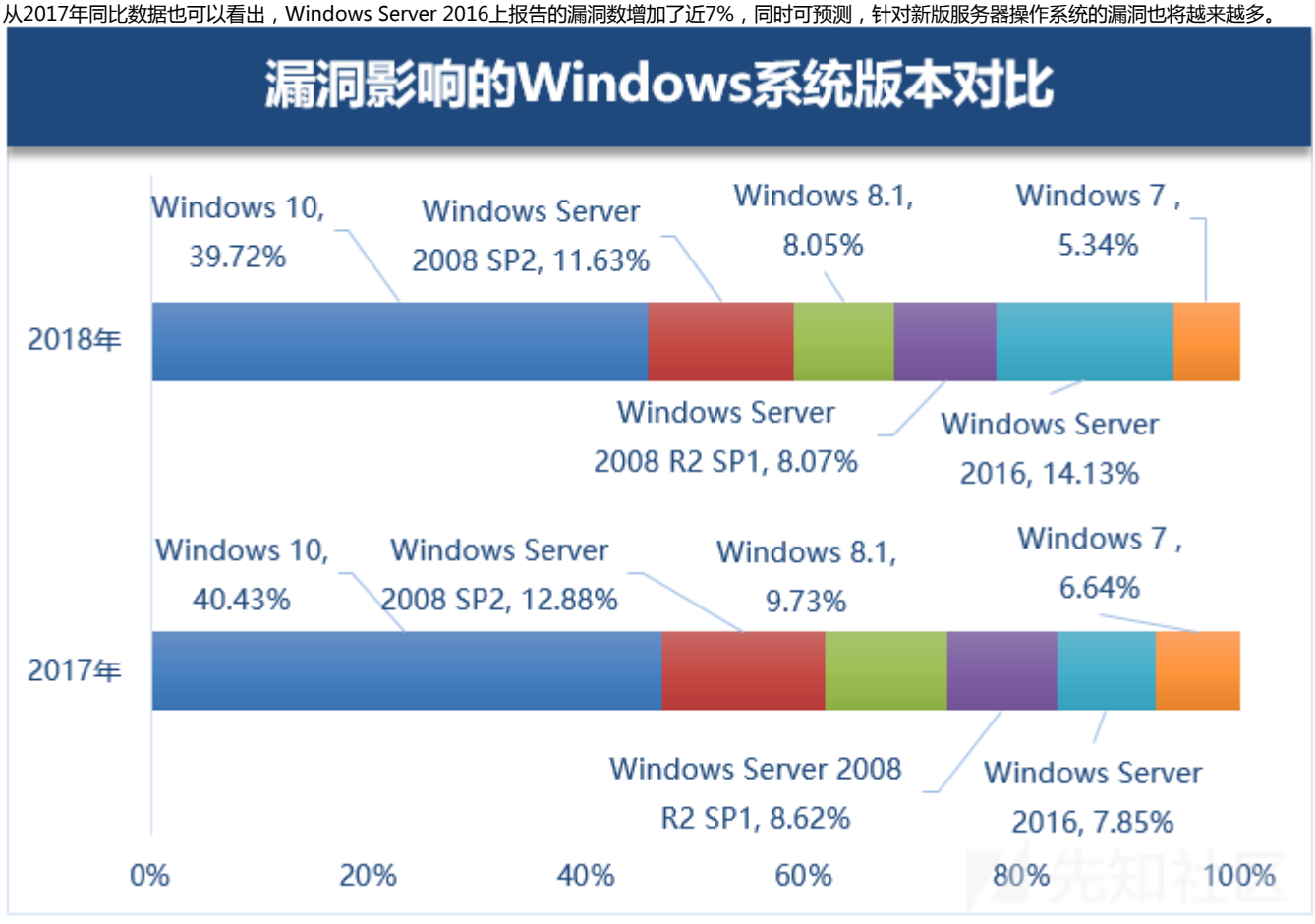
相比较2017年，2018年Office和.net的漏洞曝光量上升比较明显，相对Windows系统组件漏洞，Office漏洞常被大家忽视，但却备受黑客喜爱，众多专业黑客组织对重要目



在所有Windows各版本中，受到最多漏洞影响的却是Windows 10系统，这说明Windows
10已是主流的操作系统版本，其漏洞曝光量正越来越多，同时提醒广大用户，即便使用最新版本的操作系统，也不可忽视漏洞风险，每个月及时安装安全更新是防范黑客入

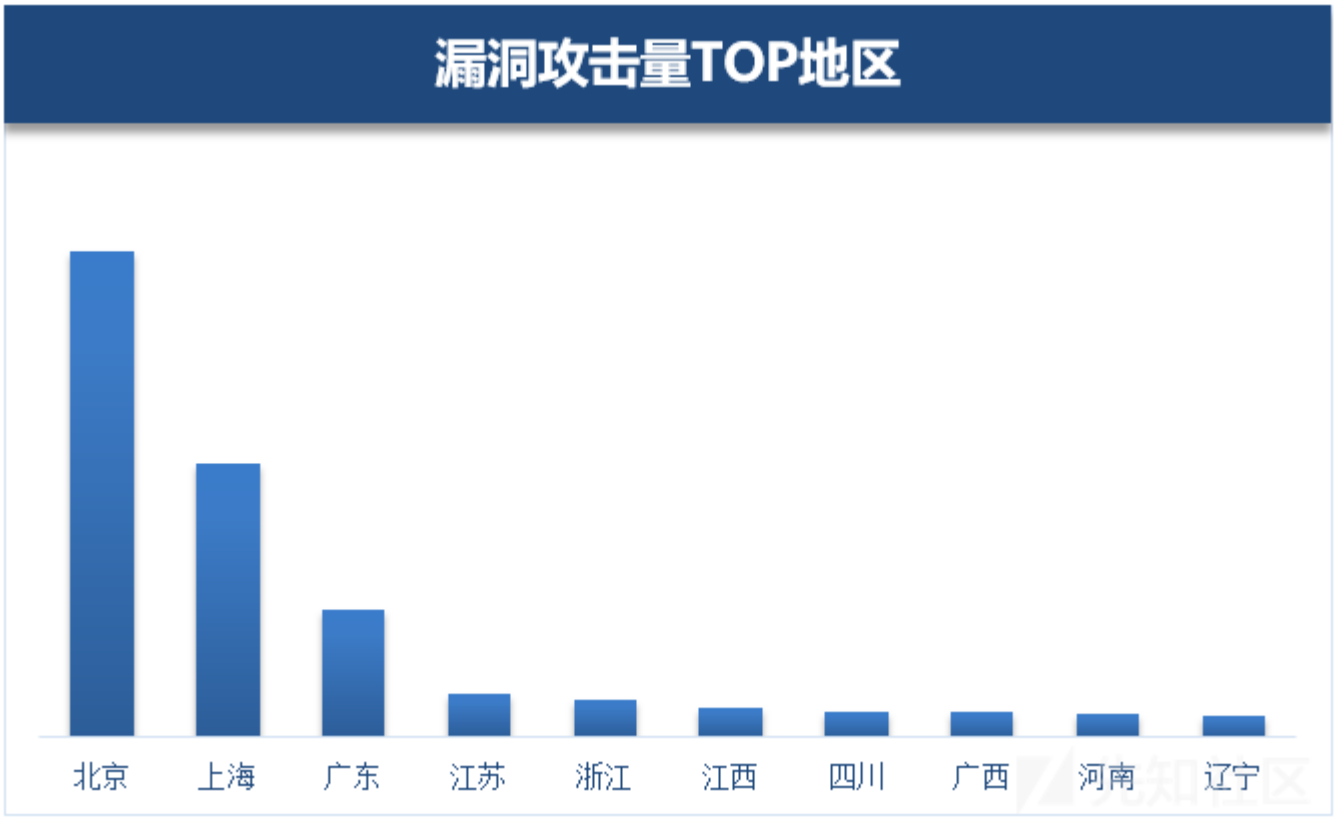


从2017年同比数据也可以看出，Windows Server 2016上报告的漏洞数增加了近7%，同时可预测，针对新版服务器操作系统的漏洞也将越来越多。

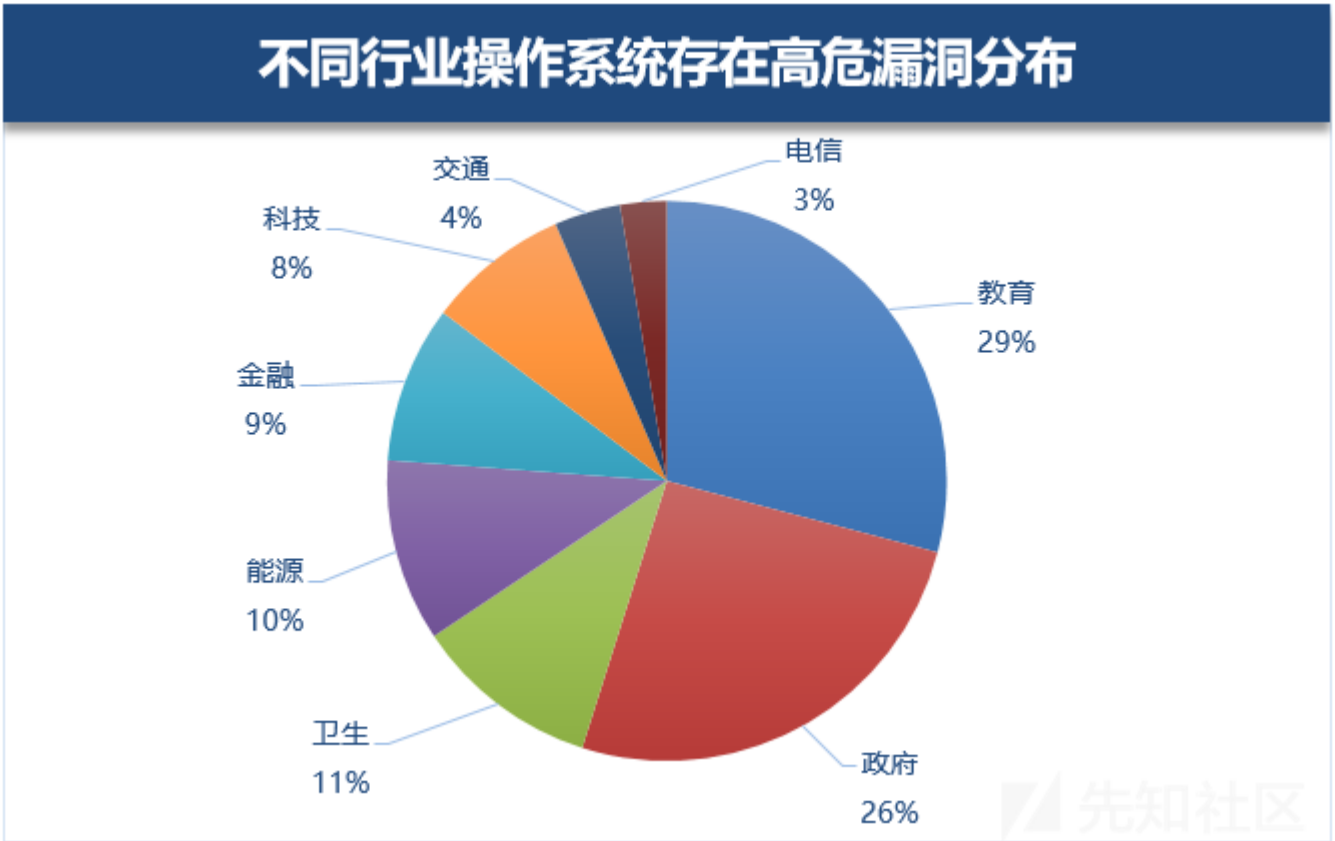


2.3 2018年漏洞攻击的地区&行业分布

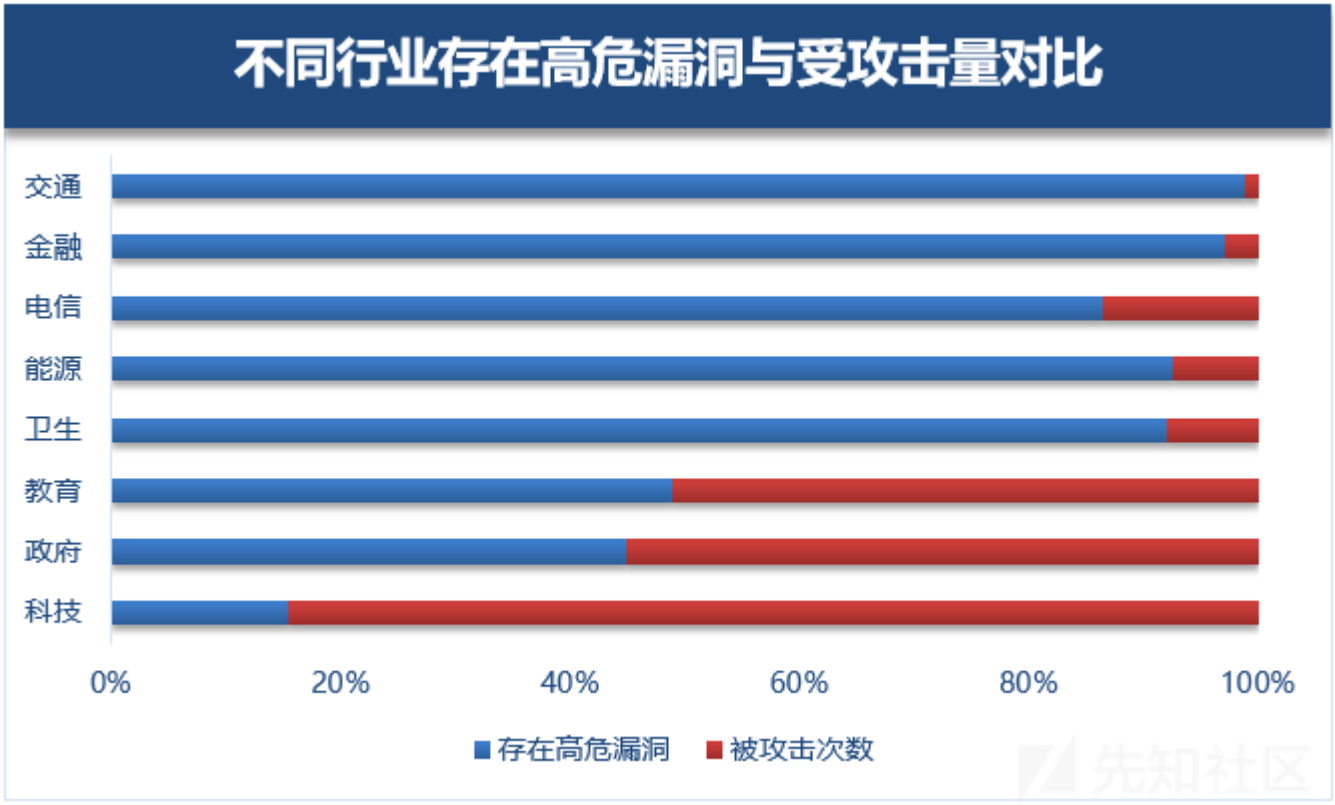
2018年漏洞攻击地区分布与当地经济水平及信息化普及程度相关。2018年漏洞攻击集中在北上广三地，其中以国家政府机关、高科技人才和经济富裕人士汇集的首都北京首



根据腾讯御见威胁情报中心数据监测， Windows操作系统存在高危漏洞在教育、政府、卫生医疗行业占比最高。

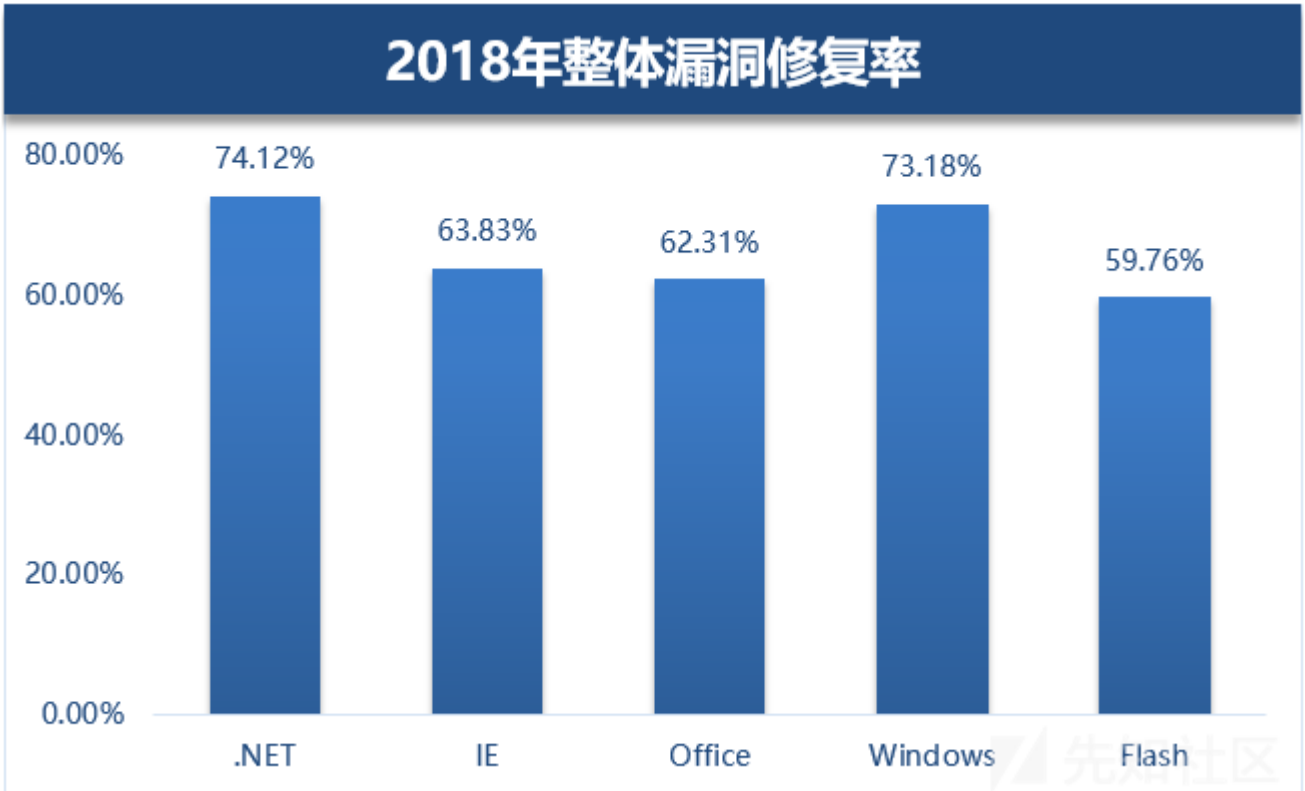


从受攻击量的对比数据看，政府、教育、医疗卫生行业因为其系统存在大量高危漏洞未及时修复，所受攻击次数也相对较高。而科技行业虽然漏洞存在量相对较少，受攻击量

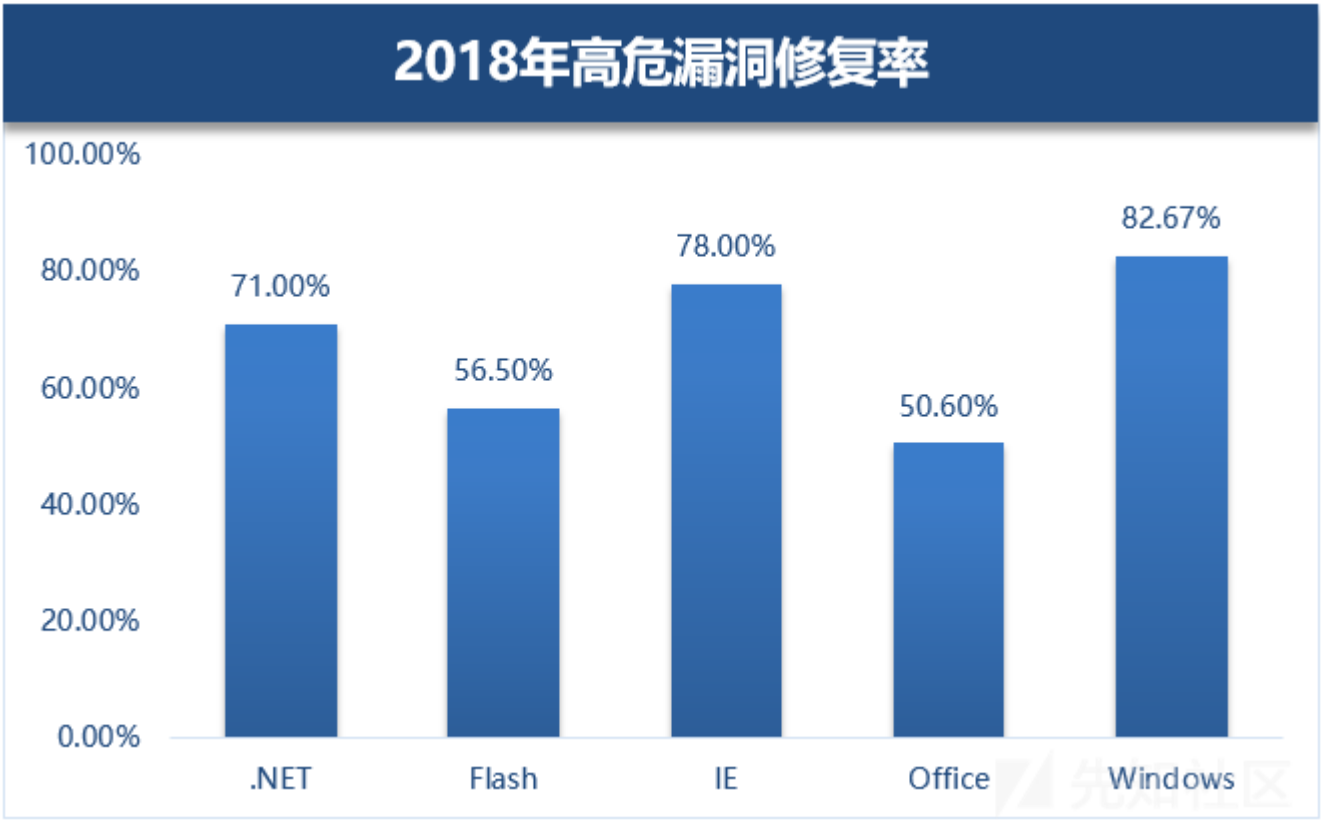


2.4 国内用户整体漏洞修复情况&高危漏洞修复情况

2018国内用户整体漏洞修复中，Windows漏洞和.NET漏洞达到了70%以上的修复率，其次是IE、Flash和Office漏洞修复率徘徊在60%上下。整体漏洞修复率偏低可以反映出



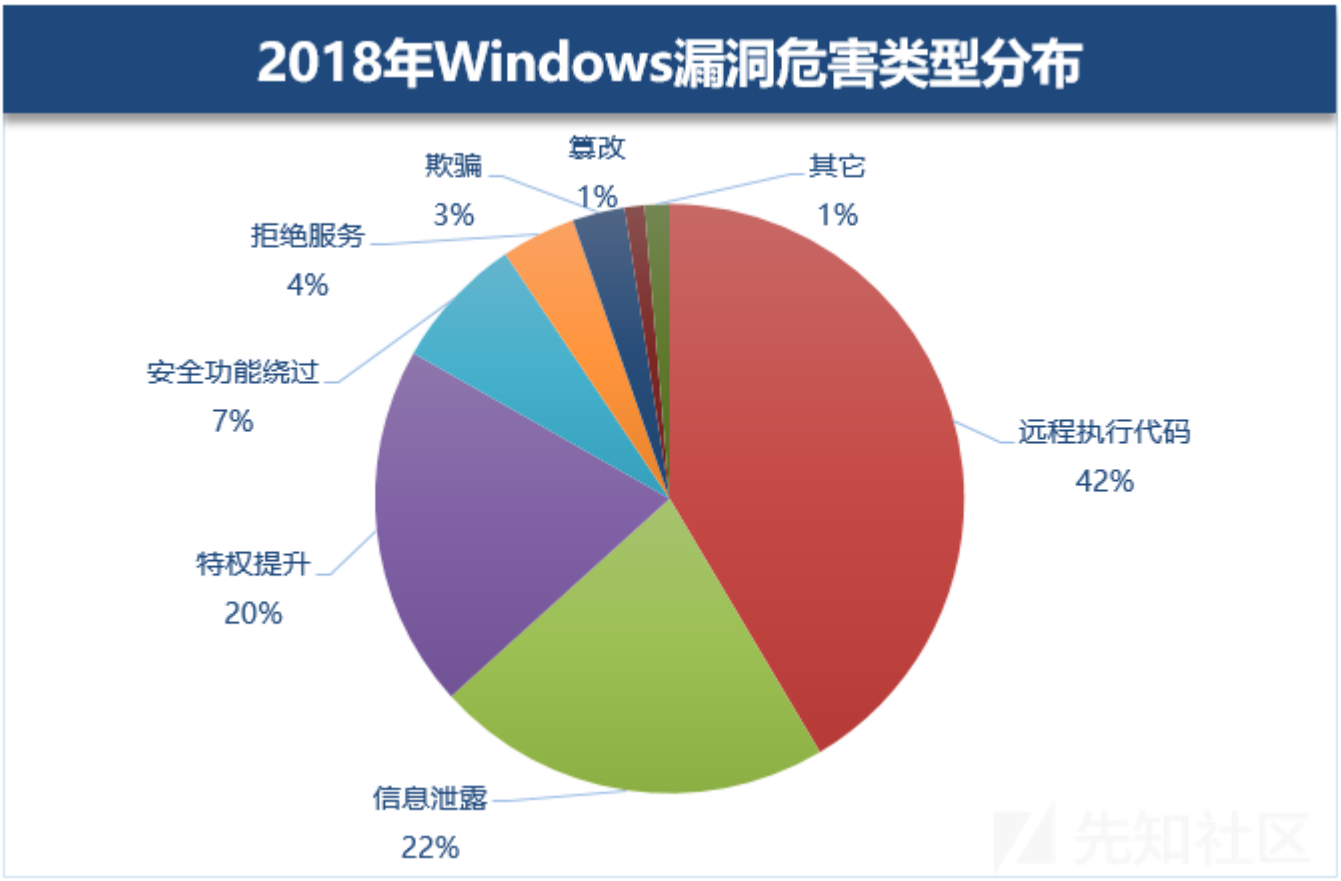
而在四类高危漏洞（存在野外利用的漏洞）修复中，Windows高危漏洞达到了82%的修复率，其次是IE和.NET高危漏洞修复率约达到70%，Flash和Office高危漏洞则修复率



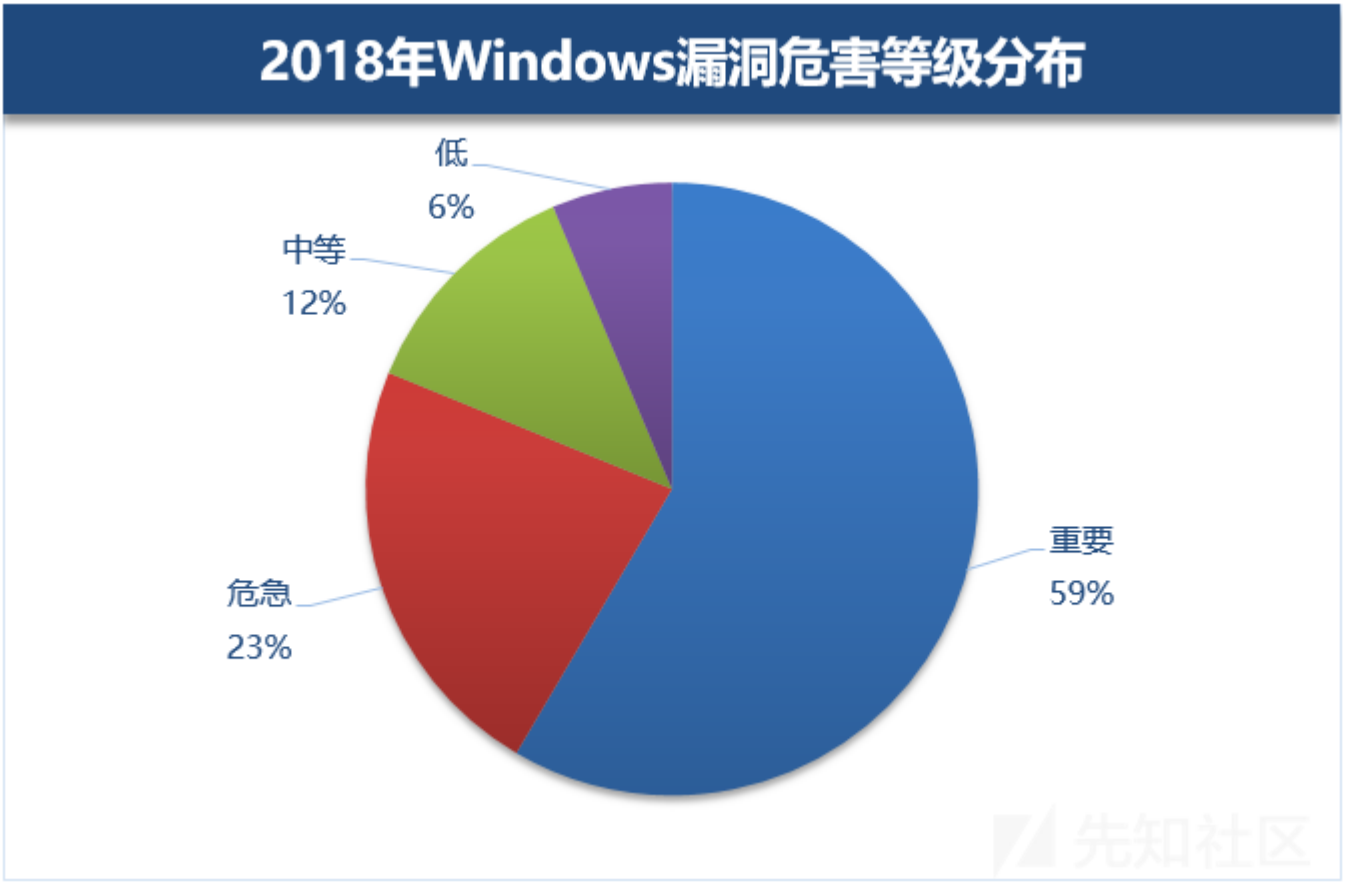
Flash高危漏洞修复率偏低是由于许多第三方软件会自带一个Flash插件，而微软官方提供的Flash补丁仅能更新其中一小部分，无法完全覆盖第三方浏览器目录下的所有Flash
Office软件本身对更新做的是相对较弱的提示，如果没有第三方安全软件的强提醒，一般用户主动安装补丁修复Office安全漏洞的较少；另一方面，国内存在大量盗版Office

2.5 Windows漏洞危害类型分布&漏洞危害等级分布

在2018年曝光的Windows平台漏洞中，远程执行代码类漏洞达到了42%的高占比，其次是信息泄露类漏洞和特权提升类漏洞各占20%。远程执行代码类漏洞由于其兼具隐蔽

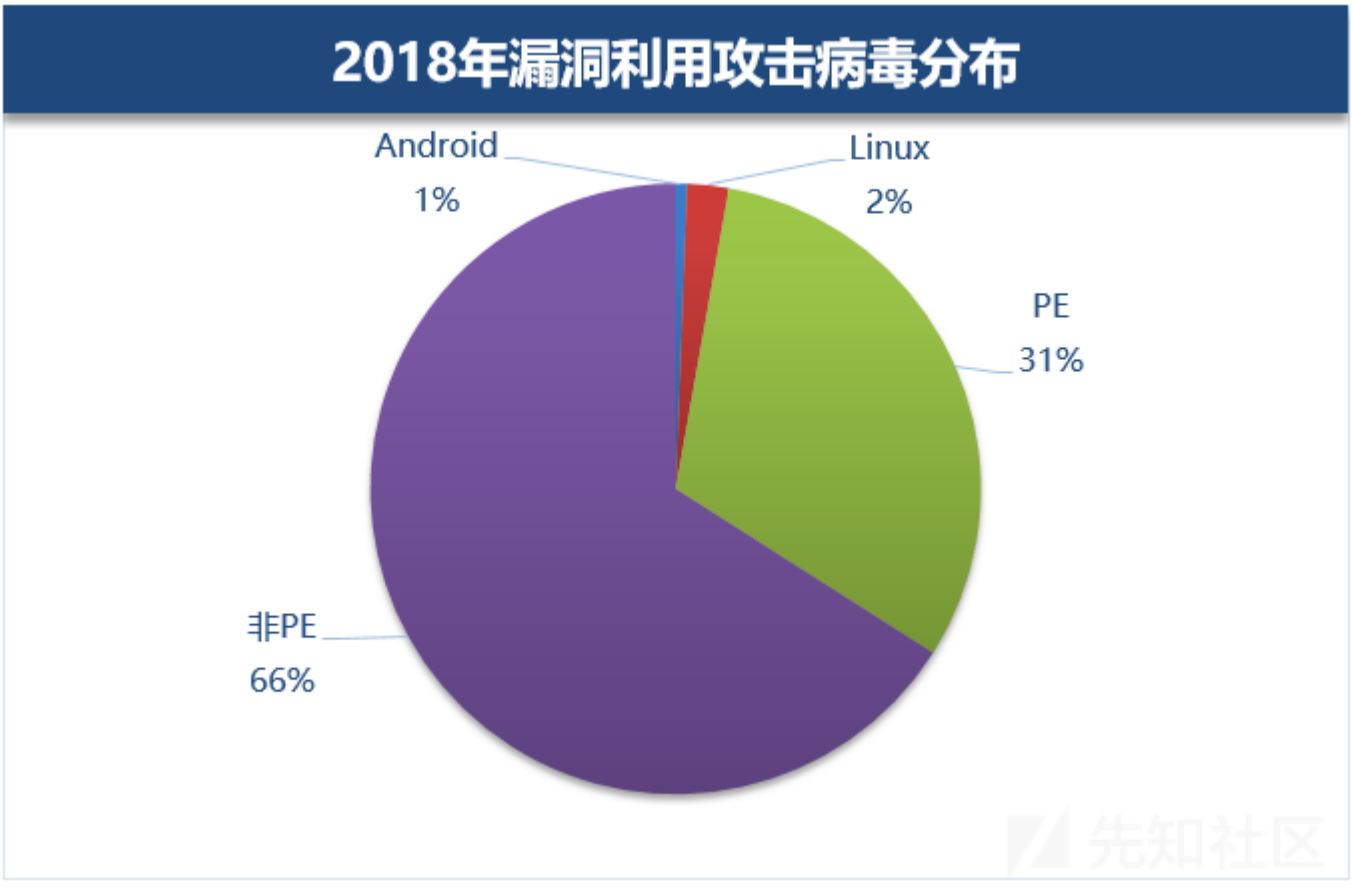


2018年曝光的Windows平台漏洞中，“危急”等级(漏洞危害最高等级)的漏洞占比23%，“危急”等级的漏洞量依然占据着较高的比例。



2.6 Windows漏洞利用病毒分布&被利用的漏洞分布

在2018年利用漏洞进行攻击的病毒中，非PE（文件格式）占了66%的高比例，而PE文件占了31%。常见非PE漏洞攻击病毒有Office宏类病毒、脚本类病毒。相比较PE，非P



2.7 2018年Windows平台高危漏洞盘点

2018年1月，Microsoft Office公式编辑器再次曝出两个高危漏洞CVE-2018-0798和CVE-2018-0802。CVE-2018-0798是Office公式编辑器在解析Matrix Record(0x05)的内容时，没有对行与列的成员进行特定的长度校验，这就导致黑客可以通过精心构造内容任意指定后续读入的行与列长度，从而造成栈溢出。CVE-2018-08

2月，Adobe Flash被曝出一个0day漏洞CVE-2018-4878。该漏洞影响版本在28.0.0.137以下的Adobe
Flash，通过修改Flash脚本对象ByteArray的值至特殊长度来实现任意地址读写，实现漏洞利用，再将Adobe Flash
Player嵌入Office文档和邮件等载体中并诱使用户打开的途径快速传播漏洞，在解析ATF文件时访问内部数据结构使用了无效的指针偏移导致漏洞，成功攻击后可能会导致敏

3月，Ulf Frisk曝光了一个Windows内核提权高危漏洞Totel Meltdown(CVE-2018-1038
)。该漏洞是由微软先前发布用于修复"Meltdown"漏洞的补丁产生的新问题，补丁错误地将PML4权限设定成用户级，可以让任意进程读取并修改页表项目，该漏洞仅影响W
x64 和 Windows Server 2008 R2系统，并在3月29日被修复；

4月，Internet
Explorer被曝出一个0day漏洞"双杀"（CVE-2018-8174）。该漏洞通过VBScriptClass::Release函数中存在的缺陷访问未分配内存，从而触发漏洞达到任意地址读写的目的。

5月，Windows操作系统和Adobe Acrobat/Reader
PDF阅读器被ESET公布了两个捆绑在一起的0day漏洞。（CVE-2018-8120、CVE-2018-4990）这是源于ESET在3月捕获的用于攻击测试的一个PDF样本。CVE-2018-4990
SetImeInfoEx 未对其目标窗口站 tagWINDOWSTATION的指针成员域 spklList
的指向地址进行有效性校验，而是直接进行读取访问。这两个漏洞已在5月被修复；

6月，Windows 10被曝出一个0day漏洞（CVE-2018-8414）。这是一个Windows Shell 远程执行代码漏洞，由于Windows
Shell在某些情况下会不正确地验证文件路径，通过精心构造的恶意脚本触发该漏洞，可以达到任意读写的目的。该漏洞仅适用于Windows
10的新文件类型".SettingContent-ms"，该漏洞直到8月14日才正式分配CVE编号并修复。

7月，Internet
Explorer被曝光0day漏洞"双杀"二代（CVE-2018-8242），它的出现是由于4月"双杀"一代（CVE-2018-8174）的修复补丁并未完全解决漏洞，导致VBScript脚本引擎中仍

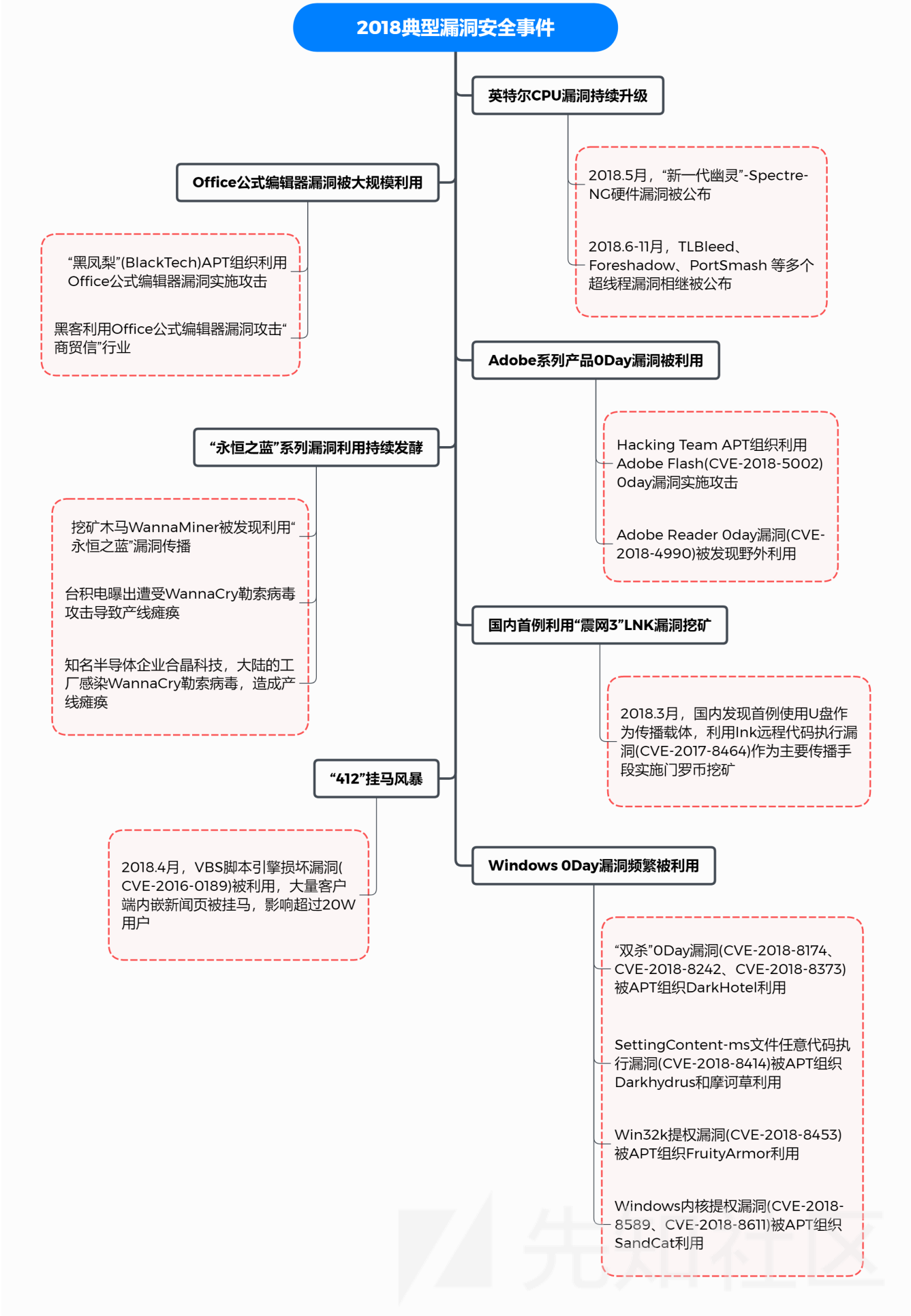
8月
(1) Exchange
Server被公开了一个内存损坏漏洞（CVE-2018-8302）的POC，攻击者可使用钓鱼攻击触发漏洞利用攻击企业用户计算机，并再次发起攻击直至接管Exchange
Server服务器。Exchange对语音邮件的接收存储过程中，会转换语音邮件读取TopNWords.Data并通过.NET
BinaryFormatter对它反序列化，该漏洞就存在于反序列化过程中。
(2) Internet
Explorer被Trendmicro曝出0day漏洞"双杀"三代（CVE-2018-8373），它基于与"双杀"一代相似的原理，通过VBScript.dll中存在的缺陷获取任意读取权限。两例漏洞都于
9月
(1)
Windows被曝出ALPC提权0day漏洞（CVE-2018-8440），它通过高级本地过程调用(ALPC)函数中SchRpcSetSecurity函数无法正确检查用户权限的缺陷，获得本地权限提
(2) Microsoft Jet Database
Engine被公开了一个远程代码执行0day漏洞（CVE-2018-8423）的POC，该漏洞是一种越界（OOB）写入漏洞，可诱导用户打开包含以JET数据库格式存储的数据的特制文
10月
(1) Microsoft Edge被公开了一个关于Windows Shell的RCE高危漏洞（CVE-2018-8495）的POC，攻击者可以使用该漏洞利用POC，通过Microsoft
Edge构造包含特殊URI的网页，诱导用户打开即可实现在远程计算机上运行恶意代码。漏洞是由于Windows
Shell处理URI时，未过滤特殊的URI所导致（如拉起脚本的Windows Script Host的URI为wshfile）。
(2)
Windows被曝出一个Win32k提权0day漏洞（CVE-2018-8453），它的利用过程较为复杂，简言之是利用了在win32k.sys组件的win32kfull!xxxDestroyWindow函数中的

11月，Windows再被曝出Win32k提权0day漏洞（CVE-2018-8589）。它的出现是由于在win32k!xxxMoveWindow函数中存在不恰当的竞争条件，导致线程之间同时发送

12月
(1) Microsoft DNS
Server被曝光存在一个堆溢出高危漏洞（CVE-2018-8626）。所有被设置为DNS服务器的Windows服务器都会受到此漏洞影响。攻击者向Windows
DNS服务器发送精心构造的漏洞利用恶意请求，以触发堆溢出并远程代码执行。漏洞于12月11日发布补丁修复。
(2)
Windows连续第四个月被曝出0day漏洞。这次是一个更加高危的kernel内核事务管理器驱动程序的提权漏洞（CVE-2018-8611），它是源于kernel模式下对文件操作的不当

三、 2018典型漏洞安全事件

2018年的安全行业，可谓是"热闹非凡"。前有勒索病毒野火烧不尽，春风吹又生；后有随着区块链概念被炒热，挖矿挂马频出；上有APT组织针对企业、政府、科研机构、事
而专业APT组织的攻击手法，对普通病毒木马黑产起到教科书般的指导和示范作用，致使高危漏洞的利用从高端到大众快速传播普及，高危漏洞对信息安全的影响力之大，由



3.1 “新一代幽灵”——英特尔CPU漏洞持续升级

继年初发现的CPU漏洞Meltdown和Spectre后，英特尔处理器在2018年5月初又被Google Project
Zero安全研究团队曝出发现8个新的“幽灵式”硬件漏洞，被称为“新一代幽灵”——Spectre-NG。利用该漏洞可绕过云主机系统与虚拟机的隔离，实现虚拟机逃逸，窃取机密
然而，在下半年再次发现了英特尔CPU存在TLBleed、Foreshadow、PortSmash等多个超线程漏洞。11月初发现的PortSmash漏洞（CVE-2018-5407）影响所有支持超线
一系列的CPU漏洞，对芯片漏洞的修复同样一波三折，仓促发布的补丁带来新的风险，同时导致CPU性能下降，补丁不得不发行了多个版本，最终促使英特尔加快新一代处

3.2 Office公式编辑器再曝新漏洞，商贸信钓鱼攻击屡试不爽（CVE-2017-11882、CVE-2018-0802、CVE-2018-0798）

Office公式编辑器漏洞（CVE-2017-11882）是典型的栈溢出漏洞，存在于Eqnedit.exe组件中，该漏洞影响所有Office版本且极易利用，由于该漏洞在2017年11月14日仅
2017年12月20日，腾讯御见威胁情报中心就发现Eqnedt32模块还存在其他漏洞，同时捕获了一例“黑凤梨”（BlackTech）APT组织利用Office公式编辑器中的0day漏洞（C
2018年1月9日，Office公式编辑器再曝出新漏洞，这次Windows干脆直接通过删掉公式编辑器的途径来修复漏洞，一了百了。但漏洞补丁刚发布一周，就已开始出现多例C
2018年2月26日腾讯御见威胁情报中心捕获到doc文档样本利用了CVE-2017-11882，通过下载并运行已被公开源码的“波尼”木马，窃取用户比特币钱包文件等敏感信息。
2018年6月1日，腾讯御见威胁情报中心再次检测到针对中国进出口企业投放的，利用CVE-2017-11882的大规模“商贸信”攻击，此类攻击邮件的投放量每天达上千封之多，
由此可以预见，未来相当长的一段时间内，鱼叉攻击+简单易用又十分符合办公场景的Office公式编辑器漏洞，仍会成为备受欢迎的针对中小型企业的攻击手段之一。

3.3 Adobe系列产品多次报警，0day漏洞屡遭曝光

3.3.1 Adobe Flash再曝0day野外利用（CVE-2018-4878、CVE-2018-5002）

2018年2月1日， Adobe官方发布了安全通告（APSA18-01）称一个最新的Adobe
Flash零日漏洞被发现用于针对韩国地区的人员发起鱼叉攻击。该0day漏洞编号为CVE-2018-4878，官方已于2月5日发布补丁进行修复。漏洞公布后，随即发现大量垃圾邮

CVE-2018-5002则在2018年6月7日被发现野外利用，由APT组织Hacking
Team通过即时聊天工具或邮箱发送包含外交部官员基本工资情况（阿拉伯语）的钓鱼文档进行攻击，在诱饵文档被用户打开后在宿主进程excel中执行恶意代码，并利用假冒
该APT组织费尽心思精心构造了攻击链，并使用0day漏洞攻击政府相关部门，可见其具有一定的政治意图。

3.3.2 Adobe Reader被发现0day漏洞在野利用攻击（CVE-2018-8120、CVE-2018-4990）

2018年5月15日， ESET捕获了一个使用两个0day漏洞联合进行攻击的PDF样本，其中包括一个Adobe
Reader的0day漏洞（CVE-2018-4990）和Win32k的内核提权0day漏洞（CVE-2018-8120）。
CVE-2018-8120是Win32k特权提升漏洞，CVE-2018-4990是Adobe
Acrobat/Reader的堆内存越界访问任意地址释放漏洞，攻击样本通过CVE-2018-4990获取代码执行权限，再通过利用内核提权漏洞绕过Adobe
Acrobat/Reader的沙盒保护并实现任意代码执行。而有意思的是该样本仅是一个测试样本，两个0day漏洞还没来得及利用于攻击便已被修复。

3.4 老漏洞被反复利用，“永恒之蓝”是否真的永恒？

多数黑客进攻个人电脑和企业服务器的目的，还是从不法途径谋取利益。往往是美味的蛋糕在哪里，不法黑客的身影就出现在哪里，病毒与木马也就如影随形地进攻到哪里。

3.4.1 “永恒之蓝”系列漏洞：从勒索病毒到挖矿木马

“永恒之蓝”是一个于2017年被曝光的，存在于445端口上的SMB文件共享协议漏洞，不法分子利用此漏洞获取系统最高权限，将病毒木马等恶意软件植入Windows系统。近
“永恒之蓝”漏洞已经成为被利用程度最高的安全漏洞之一。
勒索病毒主要通过三种途径传播：漏洞利用、钓鱼邮件和广告。其中通过漏洞发起的攻击占攻击总数的80%以上，典型案例就是以利用“永恒之蓝”漏洞主动传播的蠕虫式勒索
今年3月，腾讯御见情报威胁中心就捕获一个门罗币挖矿木马WannaMiner利用“永恒之蓝”漏洞在局域网内传播，将染毒机器打造成庞大的僵尸网络，长期潜伏挖矿，国内60
今年5月，捕获一款门罗币挖矿木马“微笑”通过扫描“永恒之蓝”漏洞攻击企业服务器悄悄在后台进行挖矿。该木马从3月就开始活动，截至5月，其已经累计挖取846枚门罗币
6月1日，捕获一款Glupteba恶意代理木马利用“永恒之蓝”漏洞在局域网迅速传播，感染量激增；
今年8月，台积电曝出遭受WannaCry勒索病毒攻击导致产线瘫痪，造成25.96亿新台币损失；
8月9日，捕获蠕虫病毒bulehero利用“永恒之蓝”漏洞在企业内网攻击传播；
11月，又有一家知名半导体企业合晶科技，其位于大陆的工厂全线感染WannaCry勒索病毒，造成产线瘫痪，工厂全部停产。
由于越大型的单位和机械系统，越追求稳定性，使用的越是win7sp0、xp等微软早已停止提供更新服务的操作系统，因此存在大量无法及时修复的漏洞。而只要漏洞场景存在

3.4.2 国内首例利用“震网3”LNK漏洞实施挖矿

2018年3月，腾讯御见威胁情报中心监测到，国内首例使用U盘作为传播载体，利用lnk远程代码执行漏洞（CVE-2017-8464）作为主要传播手段的门罗币挖矿木马。
病毒样本通过利用Lnk漏洞执行恶意代码，还会自动感染其它插入的可移动磁盘。使用U盘作为传播载体，可被用来攻击基础设施、存放关键资料的核心隔离系统等，对政企
其实“震网3”这种通过快捷方式产生的漏洞本身没什么技术含量，但由于其超链接的特性能够执行系统上任意程序或脚本，自由度极高且隐蔽性强而在漏洞利用攻击中喜闻乐

3.4.3 “412”挂马风暴（CVE-2016-0189）

2018年4月12日，腾讯御见威胁情报中心监控到大量客户端的内嵌新闻页中被嵌入恶意代码，导致用户在毫无知情的情况，被植入挖矿木马、银行木马、以及远控木马等。本
可以看到，黑客们也会“偷懒”，几乎所有被大量使用的漏洞，都是那些简单易用、稳定又成功率高的漏洞。对于黑客而言，除非是为了完成一些特殊的任务，否则那些漏洞利

3.5 Windows下半年频现0day漏洞

今年是0day漏洞持续爆发的一年，Windows系产品可谓是多灾多难，不仅在补丁发布和Win10子版本升级方面BUG频出，让用户叫苦不迭；更是在短短半年时间内被连续曝

3.5.1 “双杀”0day漏洞被APT组织DarkHotel（黑店）APT组织利用（CVE-2018-8174、CVE-2018-8242、CVE-2018-8373）

2018年4月18日，首个IE“双杀”系列漏洞CVE-2018-8174的在野攻击样本被发现，由此开启了Windows下半年每月“稳定供应”一个0day漏洞的节奏。
据报道称，该样本来自一个被命名为Darkhotel(APT-C-06)的APT组织。该APT组织善于利用高危漏洞针对企事业单位进行定向攻击，窃取国家机密，DarkHotel早在年初就

在接下来的7月、8月里，Internet
Explorer又相继被曝出“双杀”二代（CVE-2018-8242）和“双杀”三代（CVE-2018-8373）0day漏洞。DarkHotel组织再度使用相同的攻击技术，利用
“双杀”三代针对企业高管、国防工业、电子工业等重要机构发起定向攻击。
除被APT组织多次利用外，“双杀”一代（CVE-2018-8174）还在6月16日被腾讯御见威胁情报中心捕获到一个木马传播利用的案例。一款名为“流量宝流量版”的软件在软件内

3.5.2 APT组织Darkhydrus和摩诃草对CVE-2018-8414的利用

2018年6月，一种关于Windows
10新引入的文件类型”.SettingContent-ms”的任意代码执行攻击技巧被公开了POC，该漏洞一遭公开就迅速被不法黑客和APT组织利用。在野外攻击中，捕获多个利用该0d
据报道，曾发现Darkhydrus使用该漏洞利用技术，用于投递DNS隧道通信攻击，另外，疑似APT组织摩诃草也曾利用该漏洞投放攻击样本。
直到2018年8月14日微软才发布相应漏洞补丁并给予漏洞编号CVE-2018-8414。

3.5.3 APT组织FruityArmor对CVE-2018-8453的利用

CVE-2018-8453是一个位于win32kfull!xxxDestroyWindow函数中的UAF远程代码漏洞，该漏洞最早在8月由卡巴斯基实验室发现被APT组织FruityArmor利用于近期的攻击

3.5.4 APT组织SandCat对两个0day提权漏洞的利用（CVE-2018-8589、CVE-2018-8611）

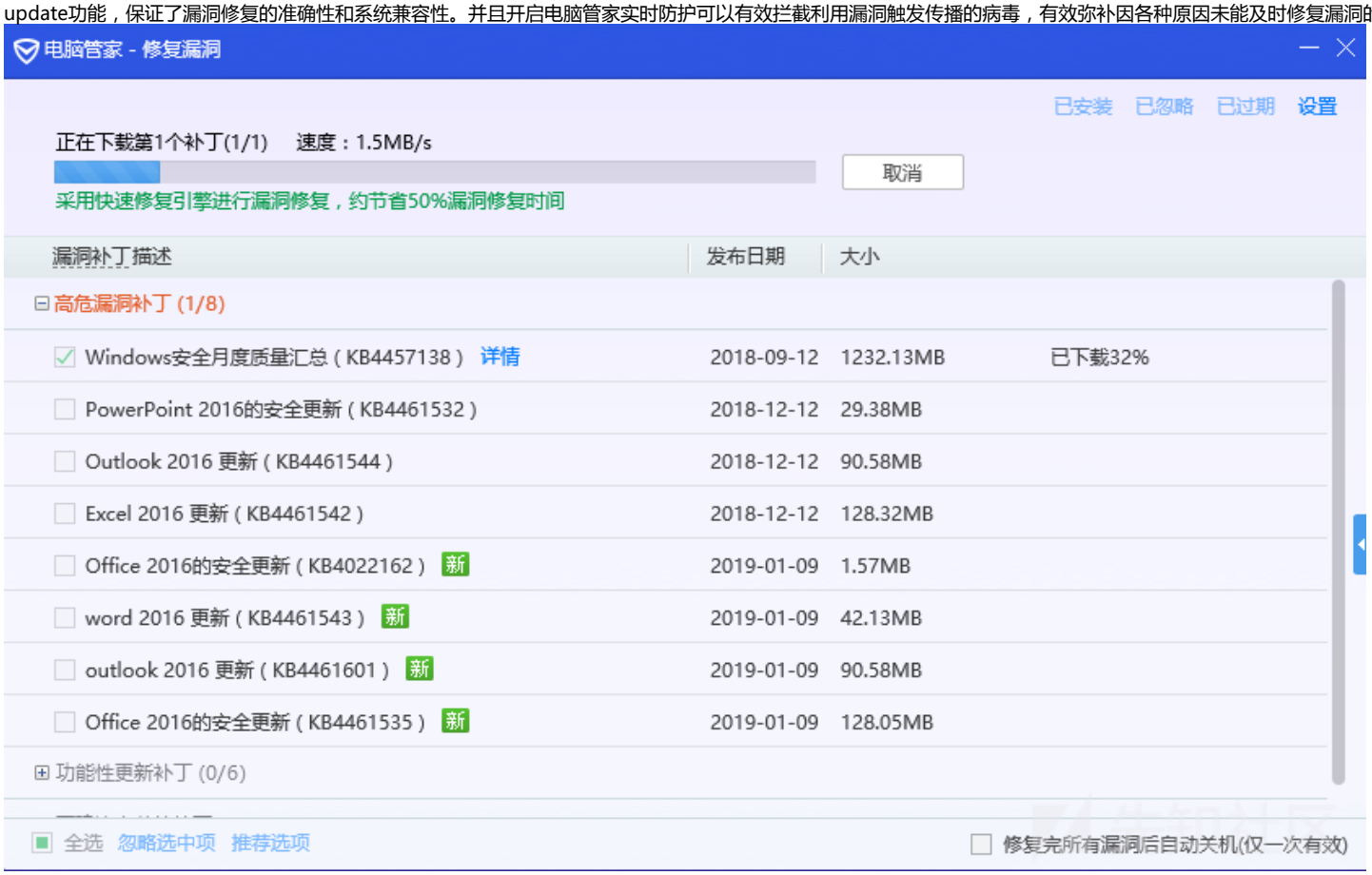
10月17日，卡巴斯基实验室发现一例APT组织SandCat针对中东地区用户进行的小范围针对性攻击，该攻击利用了Windows
Win32k本地提权漏洞CVE-2018-8589，该漏洞仅影响Windows 7 x86以及Windows Server 2008操作系统，暂时仅被发现利用于APT活动。
而该漏洞被发现还不到一个月，在10月29日，再次发现一个新的Windows内核提权0day漏洞CVE-2018-8611被同一组织利用。新的漏洞可以绕过了主流web浏览器的沙箱
Windows下半年被曝出的0day漏洞，几乎都是通过APT组织投放的攻击样本发现，可以看出APT组织较喜爱利用0day漏洞，以达到出其不意，一击必杀的目的，且将攻击最

四、 如何做好漏洞防护

4.1. 个人用户漏洞防护

4.1.1 及时修复安全漏洞开启安全软件实时防护

防范漏洞攻击最直接有效的方法就是使用新版本的系统，并且及时修复系统环境中存在的安全漏洞。腾讯电脑管家漏洞云库收集了超过千款补丁，支持Windows，Office，I
update功能，保证了漏洞修复的准确性和系统兼容性。并且开启电脑管家实时防护可以有效拦截利用漏洞触发传播的病毒，有效弥补因各种原因未能及时修复漏洞的不足。



4.1.2 培养良好的计算机使用习惯

个人需提高计算机网络安全意识，不轻易下载不明软件程序，不轻易打开不明邮件夹带的可疑附件，注意识别&不轻易打开可疑的网站，及时备份重要的数据文件。

4.2. 企业用户漏洞防护

4.2.1 建立有效的漏洞情报监控体系，建设完善的漏洞补丁管理能力

建立起有效的安全情报监控体系，密切关注各大安全媒体如“御见威胁情报中心”的威胁情报预警。
同时需要做好生产力工具的安全管理，积极安装最新补丁，修复漏洞，时刻保证个人/企业使用的设备、软件、硬件的安全性，缩短漏洞平均存续期，可以大大减少被不法分

4.2.2 安全演练，培养员工良好的信息安全意识

定期组织企业信息安全演练，以钓鱼邮件、钓鱼网页、社会工程等拟真攻击手段来提高员工安全意识，能使员工对信息安全有更深刻的印象与认识，从终端杜绝安全威胁。

五、 回顾2018，展望2019

回顾2018，勒索病毒、挖矿木马大行其道，智能合约、智能硬件、人工智能等新技术带来新趋势的同时更带来新的安全威胁，全球各领域漏洞提交数量持续上涨而0day漏洞

5.1 思维进化，道高一丈

2018年12月，国内黑客就用一起典型的、针对软件供应链发起的攻击结合利用漏洞传播木马的安全事件（广东省深圳市某知名软件厂商软件升级通道传播木马），拉开了安

5.2 千里之堤毁于蚁穴，人永远是最大的漏洞

钓鱼、广告甚至社会工程学等传统、低技术含量的手段能够屡试不爽，成为黑客们最喜爱的传播病毒、木马的手段，恰恰说明了信息安全中最大的漏洞还是在人身上。低技术

5.3 需建设多维、立体的安全能力体系

安全漏洞涉及计算机的方方面面，企业信息安全不能再只作简单的网络隔离，更要全方位地加强企业生产力设备中网络、软件、硬件的安全性，做好补丁管理及时更新企业软

上一篇：逆向工程 - 第2部分（高级编程概念） 下一篇：逆向工程 - 第2部分（高级编程概念）

1. 0 条回复

- 动动手指，沙发就是你的了！

目录