Win7停更 网络安全风险有多大

美国微软公司14日刚宣告Windows7系统停止更新，官方停止技术支持、软件更新和安全问题的修复，国内最大的网络安全企业360公司15日就披露，一场复合利用IE浏览器和火狐浏览器两个漏洞的攻击风暴悄然突袭，这意味着国内多达六成、仍在使用Windows7系统的电脑用户无法从微软官方获得支持，将直面各类利用漏洞等威胁进行的攻击。

“双星”攻击威胁有多大？

从1月14日开始，很多使用Windows7系统的电脑用户开机时都会看到“Windows7系统停止更新”的蓝色通知页面。除了关掉页面外，不少人都对此不以为然。但看不见的威胁已经到来。根据360公司的通告，近日爆发的这场被命名为“双星”的0day漏洞攻击，采用前所未有的同时复合利用IE浏览器和火狐浏览器两个0day漏洞的模式。

360集团首席安全技术官郑文彬16日告诉记者，根据360安全大脑监测到的恶意样本，发现攻击者使用组合两个0day漏洞的恶意网页进行攻击，无论IE浏览器还是火狐浏览器打开都会中招。用户在毫无防备的情况下，可被植入勒索病毒，甚至被黑客监听监控，执行窃取敏感信息等任意操作。据介绍，如此威胁巨大的“双星”0day漏洞已疑似被活跃近十余年的半岛APT组织——Darkhotel(APT-C-06)利用。从此次截获的“双星”0day漏洞攻击来看，Darkhotel(APT-C-06)攻击技术骤然升级，已从单个浏览器0day漏洞，跃升为双浏览器0day漏洞利用，威胁与破坏性远超以往。

郑文彬强调说，这次出现的漏洞是Windows7系统停服后的首个0day漏洞。尽管这次的漏洞不是Windows7系统专属，但Windows7系统停服后不会再更新安全补丁。对Windows7系统用户来说，“双星”漏洞带来的潜在伤害难以预估。目前火狐浏览器的0day漏洞现已被Mozilla官方修复，但是IE浏览器仍暴露于“双星”漏洞攻击威胁之中。

普通用户如何应对？

毫无疑问，如果windows系统一旦出现新的安全漏洞，用户将不可避免地遭受攻击，个人、企业和相关机构都会受到影响。郑文彬建议，为了减轻Windows7系统受安全漏洞的影响和防止将来被黑客攻击，安全软件变得至关重要，首先用户需要选择能够真正抵御各类安全威胁的安全软件保护自己。在WannaCry勒索病毒横行时，多国高校以及公共部门的电脑中招，其中重要原因之一就是网络安全意识薄弱，没有及时更新系统补丁，而那些仍在使用早已停止更新服务的WindowsXP系统的用户，也没有安装可靠的安全软件。

国内知名“白帽”沦沦16日接受记者采访时分析称，Win7系统的停更对普通用户来说风险是较大的。最近微软被曝出多个远程代码执行漏洞，如CVE-2020-0609和CVE-2020-0610，虽然上述漏洞不是针对Win7系统的，但也可以看出停更对于Win7今后的安全性影响还是比较大的。Win7停更给普通用户带来的主要安全风险是未知安全漏洞的利用与攻击，比如像之前的MS17010这种0day级别的漏洞，普通用户被侵入的风险就会比较大。

沦沦解释称，Win7停更之后的具体安全风险，还要取决于新漏洞的影响和利用范围。事实上，Windows系统每年都会有一些安全问题爆出，漏洞是修不完的。举例而言，微软更新的某个功能就有可能存在漏洞，也有可能微软的某个软件出现漏洞，可以和Win7系统进行结合利用等。

沦沦表示，普通用户目前需要做的就是及时更新杀毒软件，平时上网安装的软件最好都去官网下载使用，关闭高风险端口。一般还是建议把系统更新为Win10，这样会更好地保护系统不被人利用漏洞侵入。对于企业和机构用户而言，目前微软公司还会提供安全更新，但在未来有可能也会遇到停更，用户的风险也增加了。

郑文彬表示，更根本的解决方案是用户尽快升级到Win10操作系统，这样能得到微软官方更好的安全支持。

针对这次“双星”漏洞攻击事件，360公司提醒说，请勿随意打开未知来路的office文档。尤其是Windows7系统用户，应及时做好准备、全力应对系统停服后带来的安全问题，可通过权威网络安全公司提供的Win7安全防护措施提升电脑安全性。同时，提醒各相关企事业单位，警惕利用“双星”漏洞发动的定向攻击，密切跟踪该漏洞的最新情况，及时使用安全软件防御可能的漏洞攻击。

微软也提供了应对方法。一是对于拥有一台PC还不到3年的用户，可以尝试付费升级，软件起售价139美元；二是对使用PC已达3年以上的用户，建议直接购买已经内置有Win10系统的新PC。

还会出现后续漏洞吗？

据统计，直至2019年10月底，国内Windows7系统的市场份额占比仍有近六成。微软放弃Windows7系统更新，且未联合安全厂商继续支持安全防护，这意味着庞大的用户失去了微软官方的所有支持，包括软件更新、补丁修复和防火墙保障，将直面各类利用漏洞等威胁进行的攻击。由此可能带来的后果已经有过先例：2017年5月，WindowsXP系统停服3年后，利用Windows系统SMB漏洞席卷全球的WannaCry勒索病毒，横扫150个国家政府、学校、医院、金融、航班等各领域，让世界坠入勒索漩涡。2019年5月，WannaCry爆发两年之后，堪比“永恒之蓝”的Bluekeep高危远程漏洞，再次让全球400万台主机暴露在漏洞暴风眼下。

为何操作系统的漏洞层出不穷？有没有方法能一劳永逸地解决系统漏洞问题？

这次出现的“0day漏洞”，是指系统商在知晓并发布相关补丁前就被黑客组织掌握或者公开的漏洞信息。业内著名的案例是2005年12月8日，几乎影响Windows所有操作系统的WMF漏洞在网上公开，虽然微软在8天后紧急发布了安全补丁，但就在这8天内出现了200多个利用此漏洞的攻击脚本。

由于所有软件都是人编写的，是人做的就会犯错误。相关统计显示，平均每1000行代码里会有4到6个错误。Windows7系统的代码多达数千万行，其中存在漏洞数量之多可想而知，想要彻底消除这些漏洞是“不可能完成的任务”。郑文彬表示，网络攻击无时无刻都在对系统的安全防护进行刺探，因此随时都可能暴露出新的漏洞。很难说会不会有黑客组织利用尚未公开的0day漏洞作恶或等待合适的时机再出手——比如微软宣布Windows7系统停服。值得庆幸的是，尽管黑客攻击可能会因为某个漏洞的曝光让攻击频次达到高峰，但漏洞修复后也会大幅度阻断攻击的途径，让攻击减少。

本报综合消息

两名中国游客
在冰岛南部意外身亡

新华社电 雷克雅未克消息：冰岛警方16日通知中国驻冰岛大使馆，称在冰岛南部旅游景点“飞机残骸”附近发现一男一女两具中国公民遗体，死因尚待查明。

中国驻冰岛大使馆接到电话通知后高度重视，迅速启动领事保护应急机制，向冰岛警方进一步了解情况，要求警方尽快查明死因。使馆将与有关各方保持密切联系，全力做好领事保护工作。

另据自称目击者的人士透露，死者疑似自驾游遭遇暴风雪而遇难。据冰岛媒体报道，近日接连有自驾车辆误闯危险区域，因风速太大、能见度极低而被困途中。

中国驻冰岛大使馆提醒，冰岛近日连续出现暴风雪恶劣天气及雪崩等自然灾害，严重影响游客出行安全。使馆提醒中国游客务必密切关注当地天气及道路状况，注意行车和人身安全。如发生紧急情况，请及时拨打冰岛紧急救助电话+354-112，或拨打中国驻冰岛大使馆24小时领保电话+354-8932688。

以色列宣布
组建第二个F-35战机中队

新华社电 以色列国防军16日发表声明说，以色列空军当天正式组建第二个F-35战机中队。

声明说，以色列空军16日在位于以色列南部的内瓦提姆空军基地举行了第二个F-35战机中队的组建仪式。声明说，作为世界上最先进的隐形战机之一，F-35战机是一种既可防御也可进攻的多用途战机，该战机的列装有力提升了以色列空军的作战能力。以色列持续购入美国F-35战机，表明以美之间军事合作良好。

F-35战机是美国与部分盟国合作研制的第五代多用途作战飞机，配有新型航电设备，具备雷达隐身能力。根据以美达成的协议，以色列将从美国购买共50架F-35战机。据以媒体报道，以空军目前已拥有20架F-35战机，预计今年还将接收6架。2017年12月，以色列空军拥有了第一个F-35战机中队。

中国福利彩票
七乐彩全国开奖公告

第2020008期

中奖号码	基本号码	特别号码
	01 03 05 10 12 16 20	28

奖等	全国中奖注数	青海省中奖注数	每注奖金（元）
一等奖	0	0	0
二等奖	9	0	28644
三等奖	230	0	2241
四等奖	805	6	200
五等奖	8025	33	50
六等奖	15347	45	10
七等奖	96345	399	5

全国本期销售总额：7705052元
青海本省投注额：33114元

中国福利彩票3D青海省开奖公告

第2020017期

中奖号码：4 3 4
青海省销售总额：920090元
青海省中奖情况：

奖等	中奖注数	单注奖金额（元）	中奖总额（元）
单选	450	1040	468000
组选3	228	346	78888
组选6	0	173	0
包选三全中	6	693	4158
包选三组中	1	173	173
包选六全中	0	606	0
包选六组中	0	86	0
通选一等奖	0	470	0
通选二等奖	2	21	42
和数11	0	15	0
1D	2	10	20
猜1D中1	0	2	0
猜1D中2	0	12	0
猜1D中3	0	230	0
2D	3	104	312
猜2D两同号	0	37	0
猜2D两不同	0	19	0
猜大小	0	6	0
猜三同	0	104	0
拖拉机	0	65	0
猜奇偶	0	8	0

中奖总金额：551593元

利比亚“国民军”领导人为何突访希腊

利比亚军事强人哈利法·哈夫塔尔据信将参加19日在德国首都柏林举行的利比亚问题国际会议。不过他的私人飞机16日突然出现在希腊，利比亚方面和希腊方面先前均未公布这一行程。

德国当说客

希腊电视台画面显示，哈夫塔尔抵达希腊首都雅典，下榻希腊方面安排的一家豪华酒店，在那里会见希腊外交部长尼科斯·登迪亚斯。

不愿在媒体报道中公开姓名的消息人士说，哈夫塔尔将至少停留两天，17日面见希腊总理基里亚科斯·米佐塔基斯。

16日早些时候，哈夫塔尔在他的大本营班加西接待来访的德国外交部长海科·马斯。马斯稍后告诉媒体记者，哈夫塔尔愿意出席德国主办的利比亚问题会议并维持现行停火。在土耳其和俄罗斯斡旋下，哈夫塔尔和他的对头、利比亚民族团结政府总理法耶兹·萨拉杰13日在俄罗斯首都莫斯科间接对话。两人没见面，由土俄“传话”，但停火协议没签成，哈夫塔尔提前离场。马斯后来亲赴利比亚，劝哈夫塔尔去柏林接着谈。萨拉杰先前发表声明说，他会出席柏林会议。

希腊有意见

分析人士说，哈夫塔尔突访希腊，表明双方越走越近，以抗衡土耳其及其支持的利比亚西部政权。

2011年卡扎菲政权被推翻后，利比亚陷入动荡，目前呈现两大势力割据对峙局面。得到联合国承认的民族团结政府控制西部部分地区，哈夫塔尔领导的“国民军”与国民代表大会联手控制东部和中部地区、南部主要城市及部分西部城市。

一些外国媒体认为，“国民军”获俄罗斯、法国、埃及、沙特阿拉伯、阿拉伯联合酋长国支持，民族团结政府则得到卡塔尔、土耳其、意大利力挺。

土耳其议会本月初授权本国政府向利比亚出兵。土耳其总统雷杰普·塔伊普·埃尔多安16日说，土方已经开始向利比亚派遣军队。

与土耳其长期不睦的希腊马上站队“国民军”。希腊外长登迪亚斯一个月前访问班加西，会见哈夫塔尔。

希腊还对没有受邀参加柏林会议表示不满。希腊总理米佐塔基斯接受阿尔法电视台采访时说，把希腊排除在外“不对”，他会找德国总理安格拉·默克尔“说道说道”。

米佐塔基斯威胁，如果柏林会议不把土耳其与利比亚民族团结政府签署的一份海事谅解备忘录作废，“希腊将在欧盟行使否决权”，阻挠任何包含这一内容的政治解决方案。

土耳其与利比亚民族团结政府去年11月签订“海事管辖权”谅解备忘录，划定两国在地中海东部的边界线，遭到希腊等国指责。希腊指认土方划定的专属经济区侵占本国水域，妨碍希腊、塞浦路斯和以色列建设通向欧洲市场的地中海东部天然气管道。

新华社特稿