美国发动了“网络卢沟桥事变”！

[有理儿有面](javascript:void(0);)

**有理儿有面**

微信号 youli-youmian

功能介绍 你说是不是

2021-07-20[原文](https://mp.weixin.qq.com/s?__biz=Mzg3MjEyMTYyNg==&mid=2247536421&idx=2&sn=b99cfa1934b044c7fd63ee5431a86edc&chksm=cef61b50f9819246ba3c4d3006b51fea6986ca4660983a3b9c4cba533e2ffce0ee38fe3c48f4&scene=27#wechat_redirect&cpage=31) 发表于

收录于合集

以下文章来源于补壹刀 ，作者补刀客



补壹刀

.

为民族复兴鼓与呼，与中国崛起共荣辱





**全文共2109字，图片3张，预计阅读时间为6分钟。**

**文章转自：微信公众号《补壹刀》**



▼

***执笔/李小飞刀***

包括美国、欧盟、英国、澳大利亚、加拿大、新西兰、日本和北约在内的多国和组织19日晚突然发表联合声明，**指责中国是微软Exchange遭黑客攻击的幕后主使，还指责中国进行了一系列“恶意网络活动”，包括通过勒索等谋取经济利益。**



同一天美国三个政府部门发布的一份报告罗列了所谓中国黑客经常使用的超过50种策略、技术和方式。

美国国务卿布林肯称，“负责任的国家不会不加选择地危害全球网络安全”，英国外交大臣多米拉布更威胁要追究中国的责任。

美国国际广播公司称，此举标志着美国十年来对“中国黑客问题”出现重大升级。

拉帮结伙，搞突然袭击，美国想干什么。

为搞清楚这个问题，“补壹刀”专访了一位网络信息安全方面的权威专家。

**01**

**作为长期参与中国网络安全建设的专家，您怎么看这些事件的性质？**

专家：我个人认为，**这是由美国经过长期策划所策动的一次网络空间“卢沟桥事变”。**

为什么这么类比？我有两点理由：

其一，“卢沟桥事变”的时候，日军先是连续举行挑衅性的军事演习，然后借口一名叫清水节郎的新兵“失踪”，实际上是他外出解手走反了方向，以此为借口挑起全面事端，连冲突的第一枪都是日本人作假先放的。

而**美国政府纠合盟友制造的所谓中国网络攻击和勒索美西方，是网络空间中的清水节郎，因为中国很难进行查证，真相究竟为何，解释权都在对方手里。**美国及其盟友应该是经过的一段时间的策划和准备，可能是为全面对中国发动网络攻击制造的一个借口。

其二，“卢沟桥”事变之前，日本侵华都是局部性的，没有大规模全面战争的理由。干杀人放火的事也要考虑国际舆论压力。有了借口，全面侵华战争一开，所有的侵略行径都归于战争中去了，而且战争的责任还被栽赃到了中国头上。

以往美国境内IP对中国发起网络攻击，最大的伤害就是拒绝服务。**有了借口以后，美国就可以干更多的事，可以长期干，可以公开上升到国家行为，可以大片侵占，可以杀人越货，可以侵入进来把我们的数据都拿走。**

我个人认为，**美国进来拿走我们的数据，比网络攻击伤害造成的损失还要大。**这相当于，一家公司撬走了另一家公司合作伙伴的伤害，是远远不如拿走那家公司的客户名单的。

**02**

**美国多年来一直指责中国网络攻击，还经常有鼻子有眼的讲一些所谓的案例，我们如何反击？**

专家：**第一，我们在这个问题上是非常理性的，而美国是赤裸裸的“耍流氓”。**

我前面提到，“以往美国境内IP对中国发起网络攻击”，我没有直接说是美国发起攻击，而是来源于美国的IP对中国发动了攻击，那么来源美国的IP是不是等于美国行为，这需要进一步的查证，不能做直接的判断，所以中国披露境外网络攻击的时候，都采取实事求是有一说一的态度。

实际上，各国遭受网络攻击都是类似，而美国的“流氓”在于，它直接把罪名就扣在了我们头上，甚至指名道姓某个部门某个组织对它策划了网络攻击，说得有鼻子有眼，在专业人士看来如同说书。

**第二，我们也利用各种场合向外做了反击发声**，我们反复说过，中国是网络攻击的主要受害者之一，美国是针对中国网络攻击的最大来源国。中国工业控制系统的网络资产遭受来自境外的扫描嗅探，日均超过2万次。

**03**

**如果美国在实施网络“卢沟桥事变”，它之前怎么打，之后怎么打？**

互联网是美国人发明的，网络勒索也是美国人发明的。**美国是世界上网络攻击手段最多，武器库最丰富的国家。每年中国遭遇的网络攻击，其中相当大一部分比例来源于美国境内IP。**

境外以往对我们进行网络攻击的手段主要有：发布恶意程序、控制服务器、拒绝服务攻击、向中国境内网站植入后门等。从安全的角度看，上述手段对我们造成危害的程度不同，比如拒绝服务，给邮箱使劲发邮件，使邮箱不能对外提供服务。或者利用邮件服务器漏洞做一些伤害性的动作，

像网络攻击勒索工具“永恒之蓝”，或者其他被曝光出来的美国攻击手段，也只是九牛一毛，可想而知美国的武器库有多丰富。



但勒索实际伤害程度并不能算大，它并不是破坏，只是给系统加了密，要赎金，赎金的代价肯定比直接破坏的代价要小。

我经常说，真正可怕的不是别人来了，搞了破坏；而是别人来了又走了，我们根本不知道。这些年随着我们网络安全意识的提高以及技术的进步，能感知到的威胁更多了。

当然网络攻击最常采取的手段可能就是拒绝服务，不要小看拒绝服务，用在发电厂和输电线路中就是停电，用在银行系统中就是取不出钱。还有就是监控信息，长期用各种手段监控，还让我们感知不到，这就更可怕。

**04**

**我们如何防御可能的大规模网络攻击，有预案吗？**

这些年我们搞“护网行动”，按模拟攻击做了预案。但主要防御的还是低烈度攻击。好比说，我们盖的堡垒是防步枪的，如果敌人用导弹甚至原子弹攻击我们，防御可能就不行了。

**所以我们要考虑到对方采取国家行为的攻击，高烈度攻击的情况。**



此外，网络攻击没有渐进的过程，一点漏了其余全漏，这也是比较麻烦的地方。

我们现在采取的办法是划等级，等级越高防御越高。真正高等级的，一般各国都采取物理隔离的手段，建内网，大不了断网。那么相对的，像伊朗核电站，西方用的就是物理U盘手段，从人员下手。

还有，如果美国攻击我们的企业，造成了伤害，我们肯定会反制。

**（图片来自网络）**





**关注公众号：**

**有理儿有面**

**理   性｜   揭   秘｜   探   讨**







### 精选留言

用户设置不下载评论