上周末，全球近百个国家和地区遭受到一种勒索软件的攻击，有网络安全公司表示，目前全球至少发生了约 7 万 5 千起此类网络攻击事件。事件发生后，受波及的多国采取应对措施，欧洲刑警组织也对“幕后黑手”展开调查。

13 号，欧洲刑警组织在其官网上发布消息称，欧洲刑警组织已经成立网络安全专家小组，对发动本轮网络攻击的“幕后黑手”展开调查。此外，欧洲刑警组织还开始与受影响国家的相关机构展开紧密合作，共同应对网络攻击威胁，并向受害者提供帮助。

据报道，电脑被这种勒索软件感染后，其中文件会被加密锁住，支付攻击者所要求的赎金后才能解密恢复。网络安全专家说，这种勒索软件利用了“视窗”操作系统的一个名为“永恒之蓝”的漏洞。

“蠕虫”来势汹汹，专家揭“勒索病毒”真面目，并提醒网民——

及时更新操作系统补丁

微软发布相关漏洞补丁

美国微软公司12 号宣布针对攻击所利用的“视窗”操作系统漏洞，为一些它已停止服务的“视窗”平台提供补丁。

英全民医疗体系电脑系统恢复正常

在本轮网络攻击中，英国 NHS，也就是全民医疗体系旗下多家医疗机构的电脑系统瘫痪。目前，除了其中 6 家外，其余约 97%已经恢复正常。英国首相特雷莎·梅 13 号发表讲话，称英国国家网络安全中心正在与所有受攻击的机构合作调查。

事实上，这次大规模的网络攻击并不仅限于英国。当地时间 12 号，俄罗斯内政部表示，内政部约 1000 台电脑遭黑客攻击，但电脑系统中的信息并未遭到泄露。同样遭到攻击的美国联邦快递集团表示，部分使用 Windows 操作系统的电脑遭到了攻击，目前正在尽快补救。西班牙国家情报中心也证实，西班牙多家公司遭受了大规模的网络黑客攻击。电信业巨头西班牙电信总部的多台电脑陷入瘫痪。

研究人员：全球损失不可估量

美国著名软件公司赛门铁克公司研究人员 13 号预计，此次网络攻击事件，全球损失不可估量。

赛门铁克公司研究人员表示，修复漏洞中最昂贵的部分是清空每台受攻击的电脑或服务器的恶意软件，并将数据重新加密。单单此项内容就将花费高达数千万美元。

据路透社报道，软件公司关于修复漏洞的高额损失并没有包含受影响的企业所遭受的损失。

我国相关部门采取防范措施

由于这个勒索蠕虫病毒的发展速度迅猛，不仅在世界范围内造成了极大的危害，对我国的很多行业网络也造成极大影响，目前已知遭受攻击的行业包括教育、石油、交通、公安等，针对这个情况，公安部网安局正在协调我国各家网络信息安全企业对这个勒索蠕虫病毒进行预防和查杀。

据公安部网安局专家介绍，虽然目前国内部分网络运营商已经采取了防范措施，但是在一些行业内网中依然存在大量漏洞，并成为攻击目标，而一旦这些行业内部的关键服务器系统遭到攻击，从而将会带来很严重的损失。

公安部网络安全保卫局总工程师　郭启全：因为它是在互联网上传播，互联网是连通的，所以它是全球性的。有些部门的内网本来是和外网是逻辑隔离或者是物理隔离的，但是现在有些行业有些非法外联，或者是有些人不注意用 U 盘又插内网又插外网，因此很容易把病毒带到内网当中。

据记者了解，这个勒索蠕虫病毒会在局域网内进行主动攻击，病毒会通过文件共享端口进行蠕虫式感染传播，而没有修补系统漏洞的局域网用户就会被病毒感染。

公安部网络安全保卫局总工程师　郭启全：现在我们及时监测病毒的传播、变种情况，然后还是要及时监测发现，及时通报预警，及时处置。这几天，全国公安机关和其他部门和专家密切配合，特别是一些信息安全企业的专家，尽快支持我们重要行业部门，去快速处置，快速升级，打补丁，另外公安机关还在开展侦查和调查。

勒索蠕虫病毒真面目如何？

5 月 12 日开始散播勒索蠕虫病毒，从发现到大面积传播，仅仅用了几个小时，其中高校成为了重灾区。那么，这款病毒是一个什么样的病毒，如何传播，何以造成如此严重的后果呢？

这款勒索蠕虫病毒是针对微软的永恒之蓝的漏洞进行传播和攻击的。一旦电脑感染该病毒，被感染电脑会主动对局域网内的其他电脑进行随机攻击，局域网内没有修补漏洞的电脑理论上将无一幸免的感染该病毒。而该漏洞微软在今年 3 月份已经发布补丁，对漏洞进行了修复。

网络安全专家　孙晓骏：这个病毒利用了一个漏洞，但是我们用户没有打补丁的习惯，没有及时修复这次漏洞，这个病毒样本通过漏洞攻击了非常多的电脑。

根据网络安全公司数据统计，截止 5 月 13 日晚 8 点，我国共有 39730 家机构被感染，其中教育科研机构有 4341 家，高校成为了这次蠕虫病毒的重灾区。

网络安全专家　孙晓骏：这次病毒利用了 445 的一个重要的端口。校园网因为 ip 直连的情况，导致没有一个 nat 和防火墙来阻断对 445 端口的访问所以在校园网没有打补丁的机器就直接暴露在病毒之下了。

因为电脑蠕虫病毒有主动攻击的特性，所以每一次蠕虫病毒的传播范围都很广。然而在 5 月 12 号爆发的蠕虫病毒与以往不同，它入侵电脑后会加密电脑中图片、文档、视频、压缩包等各类资料，并跳出弹窗，被告之只有交了赎金，才能解密电脑中被加密的资料。

被感染蠕虫病毒后，不到十秒，电脑里的所有用户文件全部被加密无法打开。网络安全专家介绍，用户电脑一旦被感染这种勒索病毒，被加密的文件目前还没有找到有效的办法可以解锁。而专家并不建议用户支付赎金取得解锁。

网络安全专家　孙晓骏：加密的文件会根据病毒指引去付赎金获得密钥，但是根据目前的研究看成功的几率非常低，整个互联网安全界在积极的探索有没有办法解开这个密钥。因为它用的是高强度非对称加密的算法，这个密钥空间非常大，就算用暴力破解也需要非常长的时间，目前来看是不可接受的。

针对已经被感染病毒的用户，专家建议首先使用安全软件查杀蠕虫病毒，并保留被加密的文件，待日后网络安全公司找到有效方法后再进行解锁。　（据新华网）