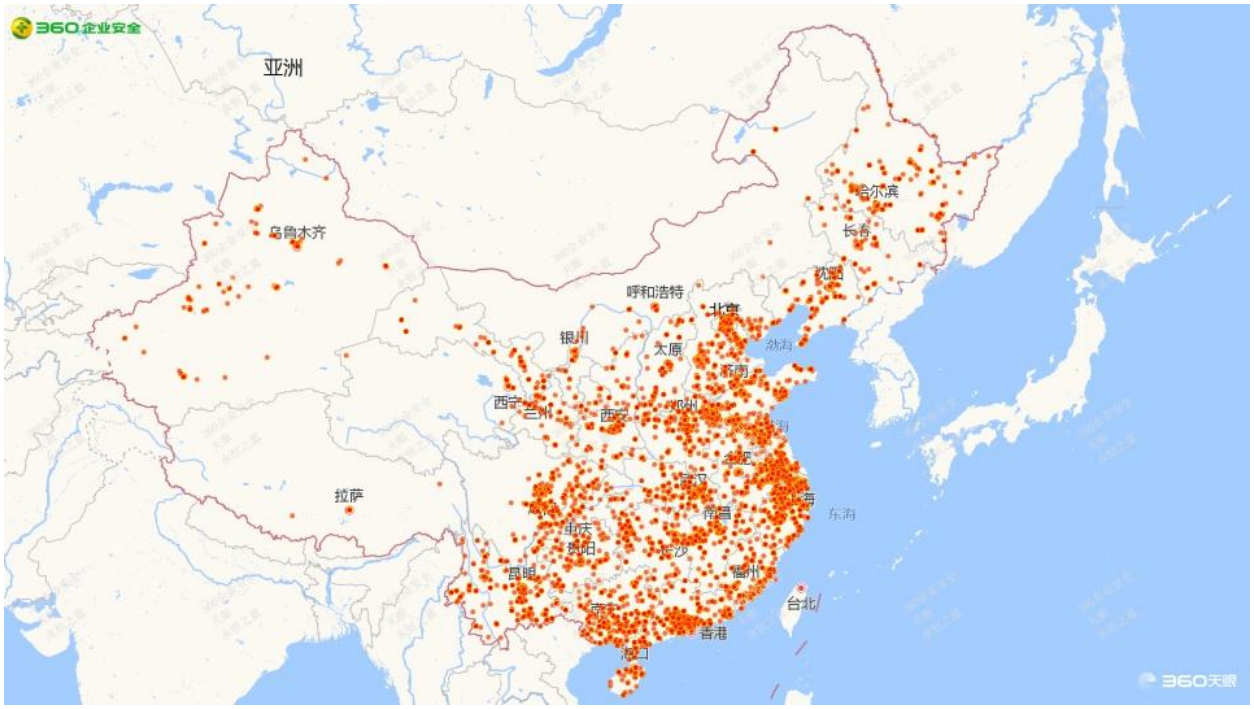
“永恒之蓝”勒索蠕虫最全知识手册

2017 年 5 月 12 日，“永恒之蓝”勒索蠕虫爆发，短短几小时，攻击了中国、英国、美国、德国、日本等近百个国家，至少 1600 家美国组织，11200 家俄罗斯组织都受到了攻击，截至到 5 月 13 日 20 点，国内也有 29372 家机构组织的数十万台机器感染，其中有教育科研机构 4341 家中招，是此次事件的重灾区，事件影响持续发酵中。



什么是“永恒之蓝”勒索蠕虫？

中了“永恒之蓝”勒索蠕虫如何紧急处置？

。。。。。。

“永恒之蓝”勒索蠕虫最全知识手册

针对大家最关心的“永恒之蓝”勒索蠕虫的相关问题

360 **企业安全专家进行专业解答，集成《“永恒之蓝”勒索蠕虫最全知识手册》**

关于“永恒之蓝”勒索蠕虫，你该知道的都在这里！

攻击原理篇

1. 什么是蠕虫病毒？

答：蠕虫病毒是一种常见的计算机病毒，它的主要特点是利用电脑存在的漏洞，通过网络进行自主的复制和传播，只要一释放出来，就会在无人干预的情况下以指数级快速扩散。

2. 这个病毒到底什么原理？

答：这个病毒是勒索软件和蠕虫病毒的合体，利用了 Windows 操作系统的一个漏洞，投送勒索软件到受害主机。在有蠕虫的环境中，有漏洞的用户电脑只要开机就会很快被感染，不需要任何用户操作，并且被感染的受害主机还会对其他主机发起同样的攻击，所以传播速度极快。

3. 中了这个病毒会有什么危害？

答：受害主机中招后，病毒就会在受害主机中植入勒索程序，硬盘中存储的文件将会被加密无法读取，勒索蠕虫病毒将要求受害者支付价值300/600 美元的比特币才能解锁，而且越往后可能要求的赎金越多，不能按时支付赎金的系统会被销毁数据。

4. 这个病毒为什么影响这么严重？

答：本次事件被认为是迄今为止影响面最大的勒索交费恶意活动事件，一旦受害主机存在被该病毒利用的漏洞，在连接网络的情况下，即使不做任何操作，病毒就会在受害主机中植入勒索程序，此外，由于其属于蠕虫病毒，具有自我复制、传播的特性，因此扩散速度极快。据 360 统计，短短一天多的时间，病毒已经攻击了近百个国家的上千家企业和公共组织，包括至少 1600 家美国组织 ,11200 家俄罗斯组织和 28388 个中国机构，全球超过 10 万家机构中招。病毒已经覆盖了国内几乎所有地区，影响范围遍布高校、火车站、自助终端、邮政、加油站、医院、政府办事终端等多个领域，被感染的电脑数字还在不断增长中。

5. 这个病毒传播面有多大，国内多少机构中招？

答：该勒索蠕虫病毒已经攻击了近百个国家，中国、英国、美国、德国、日本、土耳其、西班牙、意大利、葡萄牙、俄罗斯和乌克兰等国家的上千家企业及公共组织。据 360 威胁情报中心监测，国内至少有 28388

个机构被感染，有数十万台机器被加密勒索，覆盖了国内几乎所有地区。目前攻击事态仍在蔓延，被感染的电脑数字还在不断增长中。

6. 谁是这个病毒的制造者？

答：该病毒的制作者尚未查清，但可以确认该病毒爆发所利用的植入工具 是 4 月 14 日由 Shadow Brokers 组织泄漏的美国国家安全局(NSA)专用黑客工具，名字叫做“永恒之蓝”，是基于 Windows 网络共享协议漏洞进行攻击的。

7. 该勒索蠕虫病毒在局域网内是怎么传播的？

答：该勒索蠕虫病毒一旦被植入受害主机后，该受害主机会自动随机扫描网络内的开放 445 端口的有漏洞的其他主机，并通过 SMB 协议将勒索蠕虫病毒再植入到新的目标主机中，新的受害主机将会执行同样的动作，因此扩散传播速度极快。

8. 封闭内网的主机无法连接互联网**，是如何感染勒索蠕虫病毒的？**

答：该勒索蠕虫病毒属于蠕虫类勒索蠕虫病毒，自我复制能力极强，首次被植入的途径较多，例如有可能是已经感染的终端接入内网。

9. WannaCry 病毒除了利用 SMB 漏洞传播复制，还有其他方式吗，会通过邮件、IM 文件、U 盘传播吗？

答：此威胁可能会通过邮件、IM 文件或 U 盘发送传播，所以建议安装 360 提供的免疫工具并及时安装补丁。同时建议安装 360 天擎、安全卫士等杀毒软件，确保对该病毒的及时查杀。

360 天擎一键免疫修复工具：

10. 感染的 PC 是立即爆发还是有个潜伏期

答：该勒索蠕虫病毒一般情况下会立即生效，并会在后台进行文件加密，完成加密后将弹出勒索通知的窗口。

1. 我的电脑已经中了该勒索病毒，是否还能挽救？

答：因为勒索蠕虫病毒使用的是复杂的加密算法，理论上很难逆向破解。受害主机一旦中招，将很难通过缴纳赎金以外的方法还原文件，值得强调的是，即便缴纳赎金，一些信誉较差的攻击者也并不一定会信守承诺。

2. 我付费给勒索者，是否真的能够解密文件？

答：并不确保所有勒索蠕虫病毒攻击者在收到赎金后均会对受害主机执行解密操作。

3. 感染勒索蠕虫病毒后如何紧急处置？

答：一旦电脑中招，应首先断开已被感染主机的网络连接，隔离被感染的电脑，防止勒索蠕虫病毒进一步扩散至网内其他主机；其次是通过安装 360 天擎、安全卫士清除该病毒，并在确定病毒清除后迅速更新系统补丁；若数据价值较高，在确认攻击者信誉度后（360 可以基于所掌握的情报帮助用户评估攻击者的信誉度），可考虑支付赎金取回。

4. 用户主机中招后，免费的 360 安全卫士是否可以清除该病毒？

答：360 安全卫士已可以清除该病毒，但对于已被加密的文件无能为力。在这种情况下，可以尝试 360 公司提供的恢复工具，有可能恢复部分数据，但无法保证是最新版本。

5. 该病毒在部分用户单位的专网中正在泛滥，而很多生产主机无法执行关机操作，这种情况下如何有效抑制蔓延？

答：建议尽快将生产主机断网，待更新补丁并采取必要查杀措施后再接入网络，断网过程中，系统可保持开机状态。

1. 该病毒危害如此严重，需要打什么补丁？

答：强烈建议用户检查、安装相关的系统补丁。对于 Windows 7 及以上版本操作系统，需安装 MS17-010 补丁，微软官方下载地址为：

对 Windows XP/2003 等官方已停止服务的系统，微软已推出针对该病毒利用漏洞的特别安全补丁，下载地址为:

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

Windows XP 系统安装此补丁需要预先升级至 SP3。此外，已安装 360 天擎系统的用户，可使用其系统修复功能，对系统进行修复扫描，安装所有补丁。

在机器上线打补丁之前需要先拔除网线，暂时禁用系统上的 Server 服务，具体如何操作参照 360 企业安全提供的操作手册。

2. 是否有什么杀毒工具能够杀掉这个蠕虫？

答：目前，360 天擎、安全卫士均可查杀此病毒，但一旦该病毒在查杀前被植入，或已经成功锁定、加密用户的文件，则无法将数据恢复。以这种情况下，可以尝试 360 公司提供的恢复工具，有可能恢复部分数据。

360 公司勒索蠕虫病毒文件恢复工具：

3. 如何在主机上关闭 445 端口？

答：在 Windows 系统右键点击“我的电脑”，在“服务和应用程序”下的服务项中双击“Server”，在出现的 Server 属性页面中对“启动类

型”选择禁用，并点击“停止”按钮关闭服务。操作成功后，建议重启系统以确保生效。

4. 微软官方提供的补丁包下载地址访问速度极慢，如何解决？

答 :360 已将补丁文件打包存储至 360 云盘供用户下载 ,下载地址:（提取码：8eb0）

5. 我已安装了 360 天擎，是不是可以保证不受此病毒影响？

答：用户主机正常运行天擎，并确保开启了补丁管理模块，则可以强制网内主机及时安装补丁修复漏洞，如果漏洞修复及时，就可以避免被感染该勒索蠕虫病毒。

6. 本次事件发生在周末，大部分用户单位的 PC 均是关机状态，周一上班后该如何排查和防御？

答：可先以安全的方式下载补丁升级文件，并拷贝至确认无毒的 U 盘内，周一 PC 开机前均先断开网络连接，确认网内所有 PC 离线安装补丁后再恢复网络连接。

7. 这个病毒对 POS 机有影响吗？

答：首先确认 POS 机使用的操作系统类型，一般的移动 POS 机采用的是非 Windows 系统，因此不会受到本次病毒的感染。如果用户的特殊

设备确实使用了 Windows 操作系统，则建议联系设备供应商寻求解决方案。

8. 该病毒是否会影响 POS 机、特殊行业的手持机、工控机？机场客户的安检机和显示系统是否会受影响？该如何处理？

答：首先确认 POS 机使用的操作系统类型，一般的移动 POS 机采用的是非 Windows 系统，因此不会受到本次病毒的感染。如果 POS 机、手持机、工控机、安检机等特殊设备确实使用了 Windows 操作系统，则建议联系设备供应商寻求解决方案。

9. 为什么之前已经打了补丁还是中招了？

答：本次对应漏洞利用的补丁编号是 MS17-010，用户有可能未更新对应的补丁，尤其对于 Windows XP/2003 这类老操作系统，之前微软并没有提供安全补丁，由于本次事件影响重大才于 5 月 13 日发布了对老系统的补丁，因此必须在当前及时安装。

10. 是否有扫描工具可以检测未打补丁的主机？

答：可通过下载运行 NSA 漏洞检测工具 ，下载运行检测是否存在漏洞，但该工具不支持在服务器系统上使用。对于服务器系统，建议手工确认补丁是否已安装。目前诸如 OpenVAS 的网络漏洞扫描器可以执行远程漏洞探测功能，管理员如有需要可以使用，重点关注 MS17-010 相关的漏洞，这些漏洞被本次的蠕虫病毒所用，发现后需要及时处理。

11. 为什么我在在没有联网的情况下，开机就发现被感染了该病毒？

答：病毒是通过利用操作系统的漏洞进行传染的，如果主机开机时没有联网，很有可能是在上次关机之前已经中招。

12. 请问 Windows XP/ 2003 英文版系统是否可通过安装补丁起到防护作用？

答：可以，目前微软已经为 Windows XP/2003 提供了相应的补丁，到如下网址下载：

13. 我在网络出口已经封堵了 135/137/138/139/445 端口 ,同时安装了对应的系统补丁，是否能够有效防范该病毒，还有其他防范措施吗？

答：通过封堵端口、安装补丁，可以有效防范该病毒，但并不排除该病毒以其他形式被植入用户系统，因此建议用户安装 360 天擎、安全卫士对主机系统实现进一步防护。

14. 使用 360 提供的免疫工具后，是否可以省去安装系统补丁的工作？

答：无论是否运行免疫工具，都需要打补丁修补漏洞才可以从根本上避免被感染。此外，如果终端收到携带该病毒的文件并运行，这个终端仍旧会被感染，所以建议用户安装 360 天擎，确保对病毒执行有效防护。

15. 我们网络中部署有防火墙**设备，能起到拦截作用吗？**

答：防火墙可以起到一定的拦截作用，通过设置安全策略，阻断TCP445 端口服务，或启用防火墙的 IPS 功能，对利用该漏洞进行攻击的行为进行阻断。但是，防火墙仅能检测经过其转发的流量，对于内部主机之间的病毒传播或通过邮件等形式的传播并不能起到防护作用。最有效避免被植入该病毒的方法仍然是在系统上安装对应的补丁。