互联网网络安全信息通报

2017 年第 7 期（总第 276 期）

主办：工业和信息化部网络安全管理局

承办：国家互联网应急中心（CNCERT）　　2017 年 5 月 13 日

关于重点防范 Windows 操作系统勒索软件攻击的有关情况通报

北京时间 5 月 13 日，互联网上出现针对 Windows 操作系统的勒索软件的攻击案例，勒索软件利用此前披露的 Windows SMB 服务漏洞（对应微软漏洞公告：MS17-010）攻击手段，向终端用户进行渗透传播，并向用户勒索比特币或其他价值物，涉及到国内用户（已收到多起高校案例报告），已经构成较为严重的攻击威胁。现将有关情况通报如下：

一、勒索软件情况

4 月 16 日，CNCERT 主办的 CNVD 发布《关于加强防范 Windows 操作系统和相关软件漏洞攻击风险的情况公告》，对影子纪经人“Shadow Brokers”披露的多款涉及 Windows 操作系统 SMB 服务的漏洞攻击工具情况进行了通报（相关工具列表如下），并对有可能产生的大规模攻击进行了预警：

表 1. 有可能通过 445 端口发起攻击的漏洞攻击工具

工具名称	主要用途

ETERNALROMANCE	SMB 和 NBT 漏洞，对应 MS17-010 漏洞，针对 139 和 445 端口发起攻击，影响范围:Windows XP，2003，Vista，7，Windows 8，2008，2008 R2
EMERALDTHREAD	SMB 和 NETBIOS 漏洞，对应 MS10-061 漏洞，针对 139 和 445 端口，影响范围：Windows XP、Windows 2003
EDUCATEDSCHOLAR	SMB 服务漏洞，对应 MS09-050 漏洞，针对 445 端口
ERRATICGOPHER	SMBv1 服务漏洞，针对 445 端口，影响范围：Windows XP、 Windows server 2003，不影响 windows Vista 及之后的操作系统
ETERNALBLUE	SMBv1、SMBv2 漏洞，对应 MS17-010，针对 445 端口,影响范围：较广，从 WindowsXP 到 Windows 2012
ETERNALSYNERGY	SMBv3 漏洞，对应 MS17-010，针对 445 端口，影响范围：Windows8、Server2012
ETERNALCHAMPION	SMB v2 漏洞，针对 445 端口

综合 CNVD 技术组成员单位奇虎 360 公司、安天公司等单位已获知的样本情况和分析结果，该勒索软件在传播时基于 445 端口并利用 SMB 服务漏洞（MS17-010），总体可以判断是由于此前“Shadow Brokers”披露漏洞攻击工具而导致的后续黑产攻击威胁。当用户主机系统被该勒索软件入侵后，弹出如下勒索对话框，提示勒索目的并向用户索要比特币。而用户主机上的重要数据文件，如：照片、图片、文档、压缩包、音频、视频、可执行程序等多种类型的文件，都被恶意加密且后缀名统一修改为“.WNCRY”。目前，安全业界暂未能有效破除该勒索软的恶意加密行为，用户主机一旦被勒索软件渗透，只能通过重装操作系统的方式来解除勒索行为，但用户重要数据文件不能直接恢复。

图 1. 勒索软件界面图（来源：安天公司）

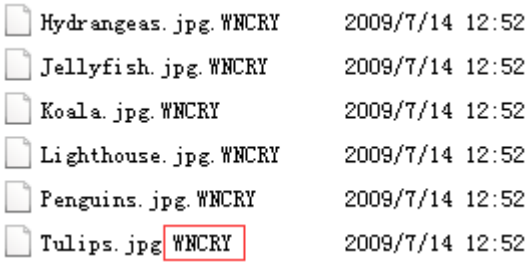

图 2. 用户文件被加密（来源：安天公司）

二、应急处置措施

根据 CNCERT 普查的结果，互联网上共有 900 余万台主机 IP 暴露 445 端口（端口开放），而中国大陆地区主机 IP 有 300 余万台。CNCERT 已经着手对勒索软件及相关网络攻击活动进行监测，目前共发现有向全球 70 多万个目标直接发起的针对 MS17-010 漏洞的攻击尝试。建议广大用户及时更新 Windows 已发布的安全补丁，同时在网络边界、内部网络区域、主机资产、数据备份方面做好如下工作：

（一）关闭 445 等端口(其他关联端口如： 135、137、139)的外部网络访问权限，在服务器上关闭不必要的上述服务端口；

（二）加强对 445 等端口（其他关联端口如：135、137、139)的内部网络区域访问审计，及时发现非授权行为或潜在的攻击行为；

（三）由于微软对部分操作系统停止安全更新，建议对 Window XP 和 Windows server 2003 主机进行排查（MS17-010 更新已不支持），使用替代操作系统。

（四）做好信息系统业务和个人数据的备份。

CNCERT 后续将密切监测和关注该勒索软件对境内党政机关和重要行业单位以及高等院校的攻击情况，同时联合安全业界对有可能出现的新的攻击传播手段、恶意样本变种进行跟踪防范。请国内相关单位做好信息系统应用情况排查工作，如需技术支援，请联系 CNCERT。电子邮箱：cncert@cert.org.cn，联系电话： 010-82990999。

报：工业和信息化部网络安全管理局

抄：工业和信息化部信息中心、中国电信、中国移动、中国联通

送：互联网网络安全信息通报工作成员单位、国家信息安全漏洞共享平台成员单位、中国互联网协会反网络病毒联盟成员单位、中国互联网网络安全威胁治理联盟
