预警编号：YJ-2017016

恒安嘉新

关于勒索软件 NotPetya 网络攻击事件

安全预警通告

恒安嘉新（北京）科技股份公司

2017 年 06 月 28 日

1 事件简介

自 2017 年 6 月 27 日开始，勒索软件“NotPetya”(Petya)的蔓延造成了一次全球性的网络攻击。此次攻击类似两个月前爆发的“WannaCry”网络攻击，两者共同之处都为利用同一个已有补丁的 Windows 安全漏洞——MS17-010 SMB 漏洞（“EternalBlue”永恒之蓝）。截止目前，乌克兰、俄罗斯、波兰、意大利、德国、法国、英国、美国等许多国家在此次事件中遭受到攻击。乌克兰和俄罗斯可能是此次事件中遭受最严重影响的国家，两国有超过 80 家公司遭到攻击。切尔诺贝利核电站的辐射监测系统在遭到攻击后离线，乌克兰的多个部门、银行和地铁系统也受到影响。

2 运行原理

“NotPetya”与两个月前爆发的“WannaCry”勒索蠕虫病毒事件不同之处在于：该病毒不再加密单个文件而是加密 NTFS 分区、覆盖 MBR、阻止机器正常启动，影响更加严重。攻击者主要通过发送携带恶意附件的邮件进行鱼叉攻击，攻击主要利用了今年 4 月份微软 Office 公布出的 RTF 执行任意代码漏洞（CVE-2017-0199），受害者遭到感染后，病毒代码会在 Windows 操作系统之前接管电脑，执行加密等恶意操作，并要求受害者支付价值约 300 美元的比特币进行解锁。与“WannaCry”类似该病毒样本运行之后，会枚举内网中的电脑，扫描 445 等端口的开放情况，并使用 SMB 协议进行连接，在存在漏洞的设备之间传播复制。

3 影响范围

理论上受到影响的 Microsoft 产品包括了所有未升级 MS17-010 补丁的操作系统版本：

Windows XP

Windows Vista

Windows 7

Windows 8

Windows 10

Windows Server 2008

Windows Server 2016

……

4 修复建议

- 本次勒索软件首次传播主要方式通过邮件进行，因此应该警惕钓鱼邮件，不要打开不明邮件中的附件或超链接。
- 更新操作系统补丁 MS17-010：

  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- 更新 Microsoft Office/WordPad 远程代码执行漏洞补丁

  (CVE-2017-0199):https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
- 避免操作系统使用空口令和弱口令，及时设置密码复杂度足够健壮的口令。

- 禁用 WMI 服务，通过在找到“控制面板”-“管理工具”-“服务”-“Windows Management Instrumentation”服务项，右键属性禁用改项服务。