1. 缓解及防御措施
2. 通过天擎控制台下发免疫工具(OnionWormImmune.exe)到终端，没有部署天擎的终端手动运行免疫工具(OnionWormImmune.exe)；运行后会自动写入注册表run项以便下次自动启动；（免疫工具的基本原理是抢占勒索蠕虫的内核对象迫使此病毒无法运行）
3. 天擎控制台升级最新的流行木马库，同时将下列文件md5在控制台和鉴定中心加黑；

MD5: 73095B7A1A52AA072DE7DB2DA8FF0496

SHA1: 4D28112AFE26A1F885AF6E2E6C0365E1273F48D3

MD5: 84C82835A5D21BBCF75A61706D8AB549

SHA1: 5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467

MD5: 4FEF5E34143E646DBF9907C4374276F5

SHA1: 47A9AD4125B6BD7C55E4E7DA251E23F089407B8F

MD5: 8495400F199AC77853C53B5A3F278F3E

SHA1: BE5D6279874DA315E3080B06083757AAD9B32C23

二、安装漏洞补丁

1. 对于微软当前支持的操作系统：Win7 SP1及以上、服务器Win2008 R2及以上，安装MS17-010、MS10-061、CVE-2017-0146、CVE-2017-0147、MS14-068、MS09-050、MS08-067漏洞补丁；对应的漏洞补丁KB号详见“微软高危漏洞-MSID与KBID对照表.xlsx”; 请确保补丁库升级到1.0.1.2823版本，该补丁库包含3月、4月、5月的高危漏洞；
2. 对于较低版本如Win7 sp0、win2008, 需要在可选补丁中安装更高的sp补丁；
3. 对于微软不再提供补丁支持的操作系统如WinXP、Win2003，只能停用server、IIS、rdp等服务，停止服务前需评估对业务是否有影响，如果有影响则通过防火墙acl严格限制出入站网络访问；

停止server服务的lua处置工具，。

附件

微软高危漏洞-MSID与KBID对照表：