“坏兔子”（BadRabbit）

勒索病毒安全预警通告

360安全监测与响应中心

2017 年 10 月 25 日

目录

第1章 安全通告

尊敬的客户：

2017 年 10 月 24 日，一款被命名为“坏兔子”(BadRabbit)的勒索软件在境外发生了一定规模的感染，目前涉及的国家主要有俄罗斯、乌克兰、保加利亚、土耳其和德国，有用户通过水坑攻击被恶意代码加密系统文件勒索要求支付赎金。作为恶意软件分发渠道而被入侵的网站包括俄罗斯的国际文传电讯社、乌克兰基辅的地铁系统、乌克兰敖德萨的国际机场以及乌克兰的基础设施部等多家大型机构。

值得注意的是，与其他通过被动方式传播的恶意软件不同， BadRabbit 通过水坑攻击将恶意代码植入到合法网站，伪装成 Flash 升级更新弹窗，诱骗用户主动下载运行恶意程序。此恶意程序除了加密受害终端的文档外，还会扫描内网 SMB 共享，使用弱密码和 Mimikatz 工具获取登录凭证等手段尝试登录和感染内网其他主机。

360 安全监测与响应中心将持续关注该事件进展，并第一时间为您更新该事件信息。

第2章 事件信息

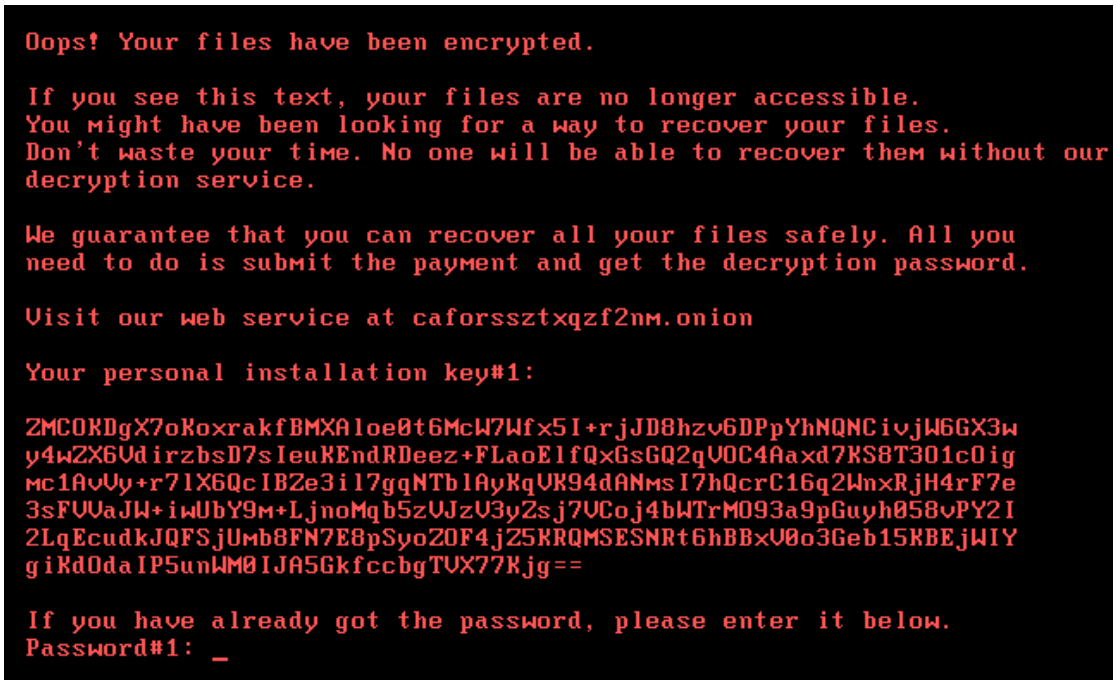
2.1 事件描述

BadRabbit 通过水坑攻击将恶意代码植入到合法网站，伪装成 Flash 升级更新弹窗，诱骗用户主动下载运行恶意程序；此恶意程序除了加密受害终端的文档外，还会扫描内网 SMB 共享，使用弱密码和 Mimikatz 工具获取登录凭证等手段尝试登录和感染内网其他主机。

BadRabbit 与 Petya/NotPetya 勒索软件有多个地方行为相同：包括使用开源的加密软件 DiskCryptor 对文档用 RSA-2048 的方式加密，和扫描内网 SMB 共享然后使用 Mimikatz 工具获取登录凭证尝试登录和感染内网其他主机。与 Petya/NotPetya 勒索软件不同的是从已知样本尚未发现通过永恒之蓝（EternalBlue）漏洞进行攻击传播。

感染此恶意软件的计算机会将用户跳转到.onion Tor 域，提示受害者需要支付 0.05 比特币的赎金（合 275 美元）解锁他们的数据。付款的网架设在 Tor 网络中，勒索信息提供支付赎金的流程，限时 40 小时，否则勒索赎金将会增加。不过支付赎金之后是否可以解密电脑文件尚不清楚。

受害者电脑会显示如下的告知支付赎金的界面：



2.2 风险等级

360 安全监测与响应中心风险评级为：高危

预警等级：蓝色预警（一般网络安全事件）

第3章 感染规模

目前，该病毒的勒索攻击范围已经蔓延到俄罗斯、乌克兰、保加利亚、土耳其和德国，包括俄罗斯的国际文传电讯社等多家大型媒体、乌克兰基辅的地铁系统、乌克兰敖德萨的国际机场以及乌克兰的基础设施部。截至目前尚未发现国内批量性的感染。

第4章 处置建议

鉴于“坏兔子”勒索病毒攻击事件已在国外发酵，并有进一步扩散的趋势，我国互联网可能受到一定程度的威胁，建议相关部门加强互联网终端防护措施，安装杀毒软件、升级病毒库，做好网络安全防护工作。

360 安全监测与响应中心不建议感染者支付赎金。首先，支付赎金并不能保证你能拿回自己的数据；其次，也是最重要的一点，拒绝支付赎金会有效阻止勒索病毒攻击的蔓延。

4.1 紧急处理措施

1、备份电脑上的重要文件到本机以外的其他机器上，检查组织内部的备份机制是否正常运作。

2、电脑安装防病毒安全软件，确认规则升级到最新。

3、关闭 WMI 服务来避免这个恶意软件通过网络散播，并阻挡 C:\Windows\infpub.dat 以及 C:\Windows\cscc.dat 文档的执行。

4、关闭不必要的网络共享。

4.2 安全操作提示

1、不要轻信网站提示弹窗和下载程序，软件更新通过安全可信渠道进行下载更新。

2、不要轻易打开包含未经请求的邮件的文件，或点开其中嵌入的链接。

3、使用高强度密码并定期更换，降低受到恶意软件感染风险。

第5章 处置建议

5.1 检测工具

360 天眼产品检测方案

1、360 天眼未知威胁感知系统和 NGSOC 产品威胁情报库的更新

360 天眼云端已经第一时间发布了该恶意样本涉及的威胁情报，请将 360 天眼未知威胁感知系统和 NGSOC 分析平台的威胁情报版本升级到最新：**2017102 51527** 或 **201710251504**。可以开启“**在线升级**”，也可以通过导入离线升级包的方式进行“**离线升级**”。同时，也可以根据公开的威胁情报在分析平台的日志搜索中进行检索，对历史感染情况进行排查。

2、360 天眼文件威胁鉴定器（沙箱）的检测方案

360 天眼文件威胁鉴定器（沙箱）在无需升级的情况下即可检测出此类样本的可疑行为。请关注文件威胁鉴定器的此类告警，并注意排查。

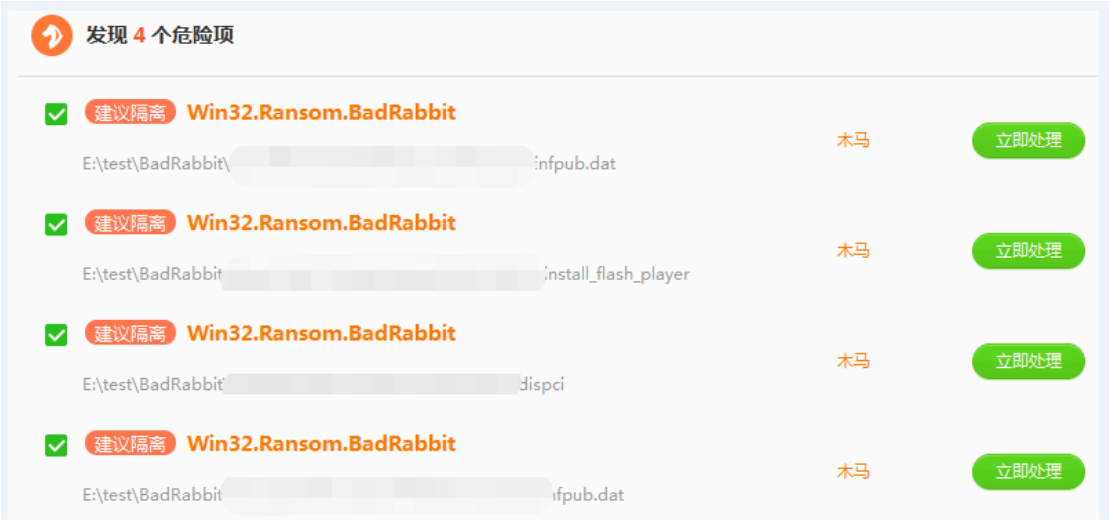
5.2 防护工具

360 天堤防火墙产品解决方案

1. 360 新一代智慧防火墙（NSG3000/5000/7000/9000 系列）和下一代极速防火墙（NSG3500/5500/7500/9500 系列）产品系列，已通过更新 IPS 特征库完成了对该勒索病毒的防护。建议用户尽快将 IPS 特征库升级至“**1710251530**”版本并启用规则 **ID: 2722** 进行防护。
2. 同时，360 新一代智慧防火墙（NSG3000/5000/7000/9000 系列）产品，已更新本地情报库。用户也可以通过升级本地情报库至“**1710251500**”版本来完成对该勒索病毒的防护。
3. 最后，使用天御云•云镜服务的用户，可以通过云镜“失陷主机”模块及时发现攻击是否已发生。

360 天擎终端安全管理系统解决方案

1. 360 天擎终端安全管理系统第一时间响应该病毒，客户终端直接连接 360 公有云查杀模式下，无需升级病毒库即可查杀该病毒。



2. 终端无法连接 360 公有云查杀模式下，需要先升级控制台病毒库版本，终端会自动同步控制台最新病毒库。控制台病毒库版本号显示为：2017-10-25。

3. 通过隔离网工具升级控制台病毒库版本。

第6章 参考文档

事件详细信息可以参考如下链接：

https://securelist.com/bad-rabbit-ransomware/82851/

https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/