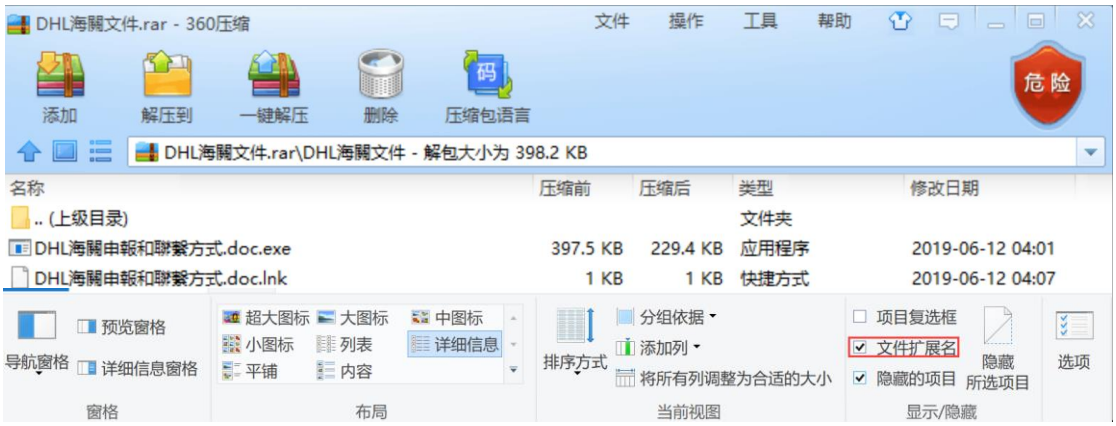
勒索病毒预警

一、事件详情

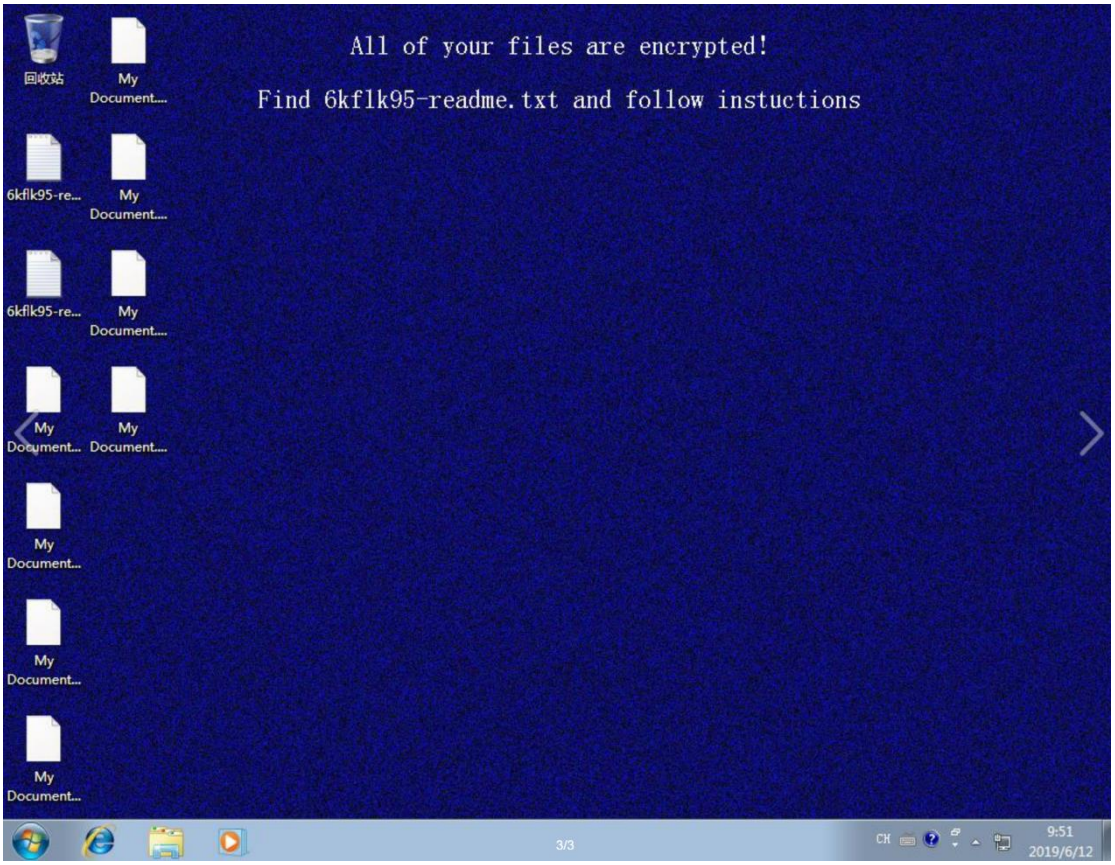
近日，多名同事的公司邮箱收到带有恶意附件的钓鱼邮件，该邮件伪装成“**DHL 货物交付延迟通知**”来获取信任，并诱使收件人打开附件。

邮件附件为压缩包，内含两个文件。在系统未勾选显示“文件扩展名”时，将显示为**.doc 文件**（实际属性为.exe 可执行文件）。



运行后，系统文件将被加密，后缀名为**.lock**。

file	c:\program files\Windows Defender\a73a6b0b.lock
file	c:\program files\Google\a73a6b0b.lock
file	c:\Users\Default\AppData\a73a6b0b.lock
file	c:\Python27\Tools\pynche\a73a6b0b.lock
file	c:\tmpd6su5a\lib\a73a6b0b.lock
file	c:\Python27\Lib\site-packages\win32\include\a73a6b0b.lock
file	c:\Python27\Lib\site-packages\socketserver\a73a6b0b.lock
file	c:\Python27\Lib\lib2to3\fixes\a73a6b0b.lock
file	c:\Python27\include\a73a6b0b.lock
file	c:\Python27\Lib\multiprocessing\a73a6b0b.lock
file	c:\Users\vbccsb\AppData\a73a6b0b.lock
file	c:\Users\Default\Links\a73a6b0b.lock
file	c:\Python27\Lib\site-packages\adodbapi\a73a6b0b.lock
file	c:\Python27\Lib\lib2to3\pgen2\a73a6b0b.lock
file	c:\Python27\Lib\test\imghdrdata\a73a6b0b.lock
file	c:\program files\microsoft sql server\110\a73a6b0b.lock



结合网上公开报告可以判断：该勒索病毒为 **Sodinokibi 勒索病毒**。Sodinokibi 最早在今年 4 月份被 Talos 发现，当时攻击者通过 WebLogic 服务器 0day 漏洞 CVE-2019-2725 发起攻击并投放该恶意负载。根据最新报告,该勒索病毒与臭名昭著的 GandCrab 勒索病毒有一定关联。由于 Sodinokibi 勒索病毒会通过电子邮件传播，因此建议不要打开任何未知来源的电子邮件，尤其是不要打开附件。即使附件来自常用联系人，也建议在打开之前，对其进行扫描，以确保它不包含任何恶意文档或文件。

现如今网络攻击事件频繁发生且具有明显的趋利性，导致挖矿木马、勒索病毒盛行。不法分子持续活跃，造成了多种潜在安全隐患，特发布病毒预警，望各部门同事提高网络安全意识，做好日常入侵检测与防御措施。

二、安全建议

（1）安装防毒杀毒软件并将病毒库升级为最新版本，并定期对计算机进行全盘扫描；

（2）不要打开任何未知来源的电子邮件，下载邮件附件后进行安全扫描；

（3）尽量关闭不必要的服务，如 SMB、SSH、RDP 等；

（4）对 3389，5900 等端口可进行白名单配置，只允许白名单内的 IP 连接登陆；

（5）采用高强度的密码，避免使用弱口令密码，并定期更换密码。建议服务器密码使用高强度且无规律密码，并且强制要求每个服务器使用不同密码管理；

（6）及时更新系统补丁，防止攻击者通过漏洞入侵系统。

2019 年 6 月 13 日