信息系统安全周报

亚信安全客户服务中心

感谢您订阅由亚信安全客户服务中心撰写的《信息系统安全周报》。
我们竭诚为您提供最新的安全资讯、病毒流行趋势、系统漏洞提示及网络安全防护技巧。

病毒情报中心		系统漏洞信息
一周病毒情况报告 亚信安全热门病毒综述- Backdoor.Linux.BASHLITE.AMF		KB4493470
系统安全技巧		**亚信安全产品**
携带加密附件的垃圾邮件预警		病毒码发布情况

一周病毒情况报告

本周用户报告感染数量较多的病毒列表

- TROJ_EQUATED 家族

亚信安全热门病毒综述

亚信安全热门病毒综述- Backdoor.Linux.BASHLITE.AMF

该病毒由其它恶意软件生成或者用户访问恶意网站不经意下载感染本机，其会连接到以下 URL 发送和接收来自远程恶意用户的命令：

- {BLOCKED}.{BLOCKED}.25.213:3437

- 对该病毒的防护可以从下述链接中获取最新版本的病毒码：14.937.60
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 病毒详细信息请查询：
  https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/backdoor.linux.bashlite.amf

系统漏洞信息

Windows 安全更新 (4493470)

Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows Server 2016

描述：https://portal.msrc.microsoft.com/zh-cn/security-guidance

亚信安全产品

病毒码发布情况

亚信安全在最近一周发布中国区病毒码情况如下：

2019 年 04 月 08 日发布病毒码 14.921.60
2019 年 04 月 09 日发布病毒码 14.923.60

2019 年 04 月 10 日发布病毒码 14.927.60

2019 年 04 月 11 日发布病毒码 14.929.60

2019 年 04 月 12 日发布病毒码 14.931.60

截至目前，病毒码的最高版本为 14.937.60 发布于 2019 年 04 月 15 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/TSUT/

趋势科技在最近一周发布全球病毒码情况如下：

2019 年 04 月 08 日发布病毒码 14.925.00

2019 年 04 月 09 日发布病毒码 14.927.00

2019 年 04 月 10 日发布病毒码 14.929.00

2019 年 04 月 11 日发布病毒码 14.931.00

2019 年 04 月 12 日发布病毒码 14.933.00

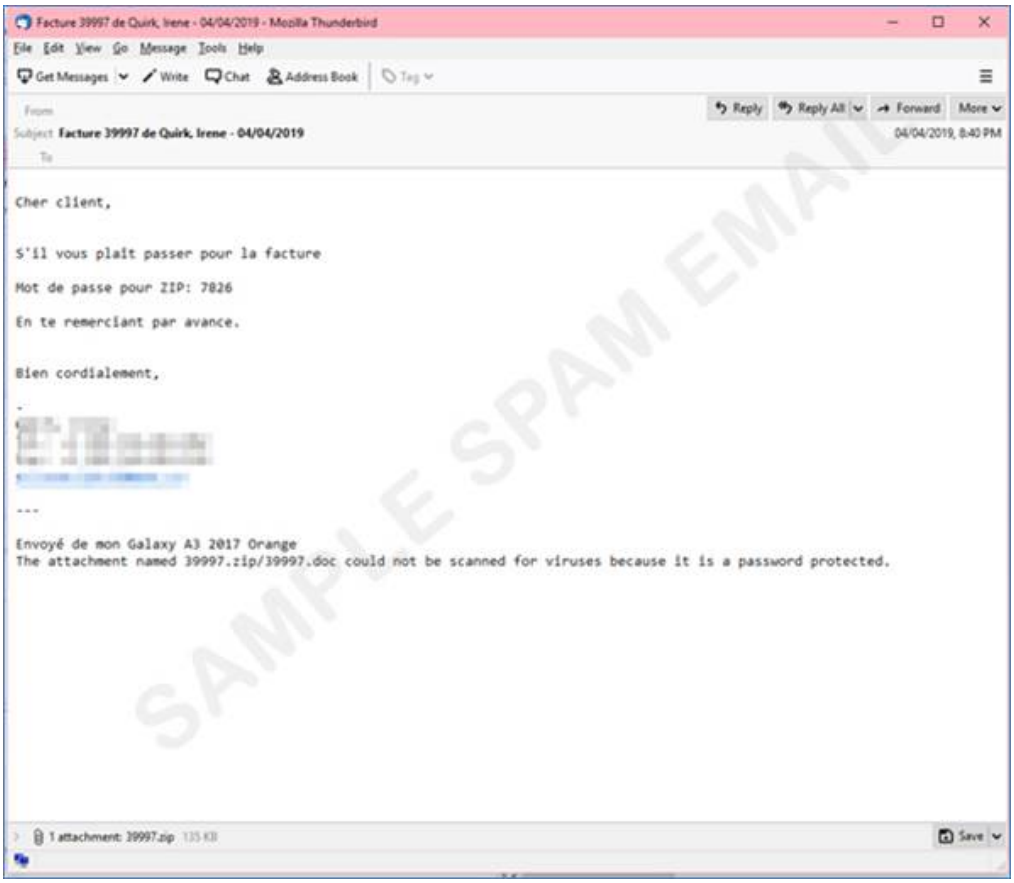
截至目前，病毒码的最高版本为 14.939.00，发布于 2019 年 04 月 15 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/Main-Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/TSUT/

系统安全技巧

近日，亚信安全截获大量使用不同语言编写的垃圾邮件，这些垃圾邮件附件携带有加密的 zip 文档，邮件正文中则注明了解密密码，诱骗用户点击附件文档。附件文档包含病毒文件，亚信安全将其命名为 Trojan.W97M.POWLOAD。

此类邮件主题通常是与发票有关，用户打开附件，输入解压缩口令后，执行压缩包内的 doc 文件，其会通过 PowerShell 下载三个随机数命名的可执行文件，亚信安全已经可以检测这些可执行文件，将其命名为 TrojanSpy.Win32.EMOTET.SMA。这些随机数可执行文件就是著名的 EMOTET 银行木马文件，其通常是通过垃圾邮件进行传播。



解决方案

- ✓ 不要点击来源不明的邮件及附件；
- ✓ 不要访问邮件中的可疑链接；
- ✓ 对邮件内容进行甄别，谨防上当受骗；

亚信安全解决方案

- ✓ 亚信安全垃圾邮件病毒码版本 24536 已经可以拦截此类垃圾邮件，请及时升级垃圾邮件病毒码版本。

- ✓ 亚信安全中国区病毒码版本 14.927.60，云病毒码版本 14.927.71，全球码版本 14.929.00 已经可以检测垃圾邮件附件中的病毒文件，请用户及时升级病毒码版本。

总结：

垃圾邮件攻击往往邮件内容都是包含一些用户关注或者是近期流行性话题，利用人们的好奇心达 到运行恶意附件的目的。我们建议用户可以通过部署网关类产品作为第一道防线，在源头上进行阻断；桌面防护产品可以有效阻止威胁到达客户端；人员安全意识培训也是必不可少的环节。