2016 年 10 月 24 日，星期一

Pumpkin 加 Locky

作者：Warren Mercer 和 Edmund Brumaghin

摘要

在先后见过 .locky、.odin 和 .zepto 之后，我们遇到了最糟糕的情形：现在，Locky 开始将 .shit 用作加密文件扩展名。在如今最新一波垃圾邮件浪潮中，Talos 研究了散布最新版本 Locky 勒索软件的三种不同的垃圾邮件活动。这种情况是在 Locky“休假”两周左右后出现的。利用 Talos 之前发布的 LockyDump 实用程序，我们得以发现这些恶意软件活动存在截然不同的特征。这些特征似乎与每个活动中的 Locky 二进制文件所关联的联属 ID 有联系。

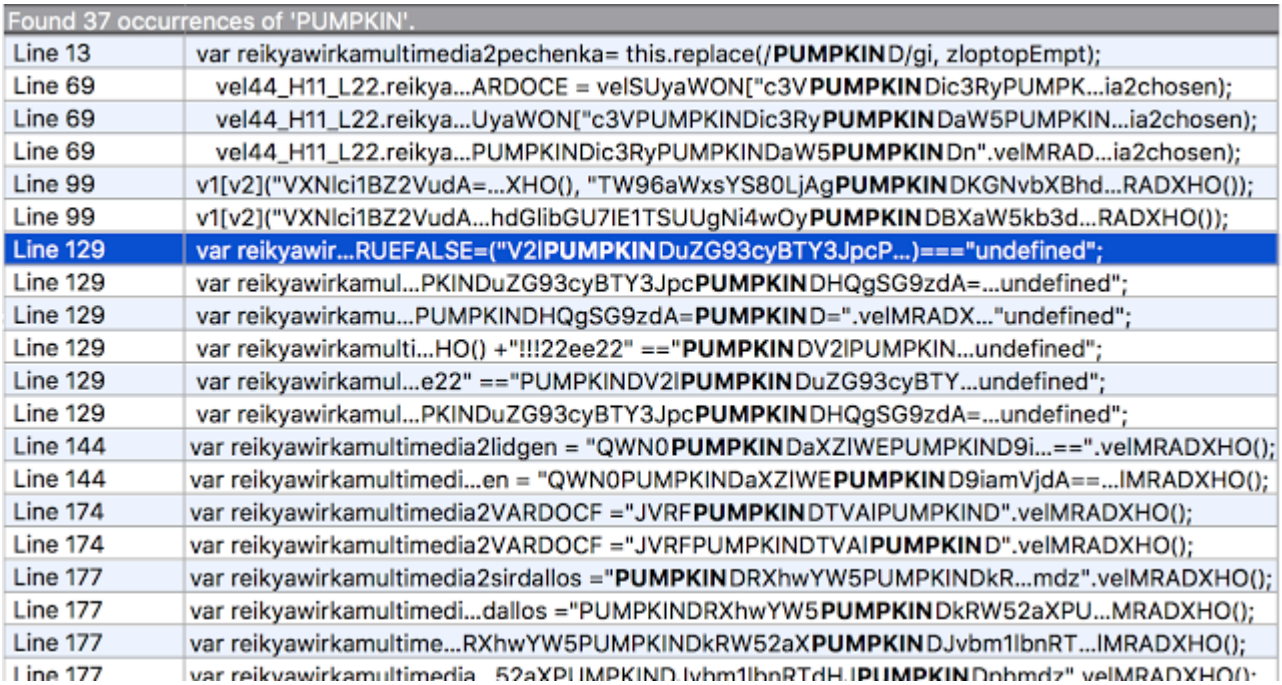
关于与 Locky 系列勒索软件相关的技术详细信息已经有大量文档和报告，因此我们不再花费时间对该系列勒索软件本身进行深入技术分析。本文将重点介绍我们研究的每个活动的特征。在本文末尾，我们还将总结所有危害表现 (IOC)。

活动详细信息

活动 1：“Receipt XXX-XXX”垃圾邮件（联属 ID=3）

该活动是今天早上（2016 年 10 月 24 日）才刚研究的，其中使用的邮件试图利用恶意 .HTA 文件作为恶意软件下载器。这些邮件忿恿收件人打开声称包含收据的消息。与此活动关联的邮件使用的主题为“Receipt XXX-XXX”，其中 XXX 是序号。HTA 文件封装在名为“Receipt XXX-XXX.zip”的 .ZIP 存档中。.HTA 文件的文件名为“Receipt XXXXX-XXXXXX.hta”，该文件一旦被打开，就会成为真正 Locky 勒索软件的恶意软件下载器。

一个有趣的现象是，.HTA 下载器所用的混淆工具反复使用基于“PUMPKIN”这个词的变量名称。在我们分析的示例中，有 37 个独立实例中出现了“PUMPKIN”。这跟即将到来的万圣节有关。



Found 37 occurrences of 'PUMPKIN'.	
Line 13	var reikyawirkamultimedia2pechenka= this.replace(/**PUMPKIN**D/gi, zloptopEmpt);
Line 69	vel44_H11_L22.reikya...ARDOCE = velSUyaWON["c3V**PUMPKIN**Dic3RyPUMPK...ia2chosen);
Line 69	vel44_H11_L22.reikya...UyaWON["c3VPUMPKINDic3Ry**PUMPKIN**DaW5PUMPKIN...ia2chosen);
Line 69	vel44_H11_L22.reikya...PUMPKINDic3RyPUMPKINDaW5**PUMPKIN**Dn".velMRAD...ia2chosen);
Line 99	v1[v2]("VXNlci1BZ2VudA=...XHO(), "TW96aWxsYS80LjAg**PUMPKIN**DKGNvbXBhd...RADXHO());
Line 99	v1[v2]("VXNlci1BZ2VudA...hdGlibGU7IE1TSUUgNi4wOy**PUMPKIN**DBXaW5kb3d...RADXHO());
Line 129	var reikyawir...RUEFALSE=("V2l**PUMPKIN**DuZG93cyBTY3JpcP...)==="undefined";
Line 129	var reikyawirkamul...PKINDuZG93cyBTY3Jpc**PUMPKIN**DHQgSG9zdA=...undefined";
Line 129	var reikyawirkamu...PUMPKINDHQgSG9zdA=**PUMPKIN**D=".velMRADX..."undefined";
Line 129	var reikyawirkamulti...HO() +"!!!22ee22" =="**PUMPKIN**DV2lPUMPKIN...undefined";
Line 129	var reikyawirkamul...e22" =="PUMPKINDV2l**PUMPKIN**DuZG93cyBTY...undefined";
Line 129	var reikyawirkamul...PKINDuZG93cyBTY3Jpc**PUMPKIN**DHQgSG9zdA=...undefined";
Line 144	var reikyawirkamultimedia2lidgen = "QWN0**PUMPKIN**DaXZlWEPUMPKIND9i...==".velMRADXHO();
Line 144	var reikyawirkamultimedi...en = "QWN0PUMPKINDaXZlWE**PUMPKIN**D9iamVjdA==...lMRADXHO();
Line 174	var reikyawirkamultimedia2VARDOCF ="JVRF**PUMPKIN**DTVAlPUMPKIND".velMRADXHO();
Line 174	var reikyawirkamultimedia2VARDOCF ="JVRFPUMPKINDTVAl**PUMPKIN**D".velMRADXHO();
Line 177	var reikyawirkamultimedia2sirdallos ="**PUMPKIN**DRXhwYW5PUMPKINDkR...mdz".velMRADXHO();
Line 177	var reikyawirkamultimedi...dallos ="PUMPKINDRXhwYW5**PUMPKIN**DkRW52aXPU...MRADXHO();
Line 177	var reikyawirkamultime...RXhwYW5PUMPKINDkRW52aX**PUMPKIN**DJvbm1lbnRT...lMRADXHO();
Line 177	var reikyawirkamultimedia...52aXPUMPKINDJvbm1lbnRTdHJ**PUMPKIN**Dpbmdz".velMRADXHO();

图 A：HTA 下载器中出现的“PUMPKIN”

针对此活动中的样本运行 LockyDump 得到以下信息：

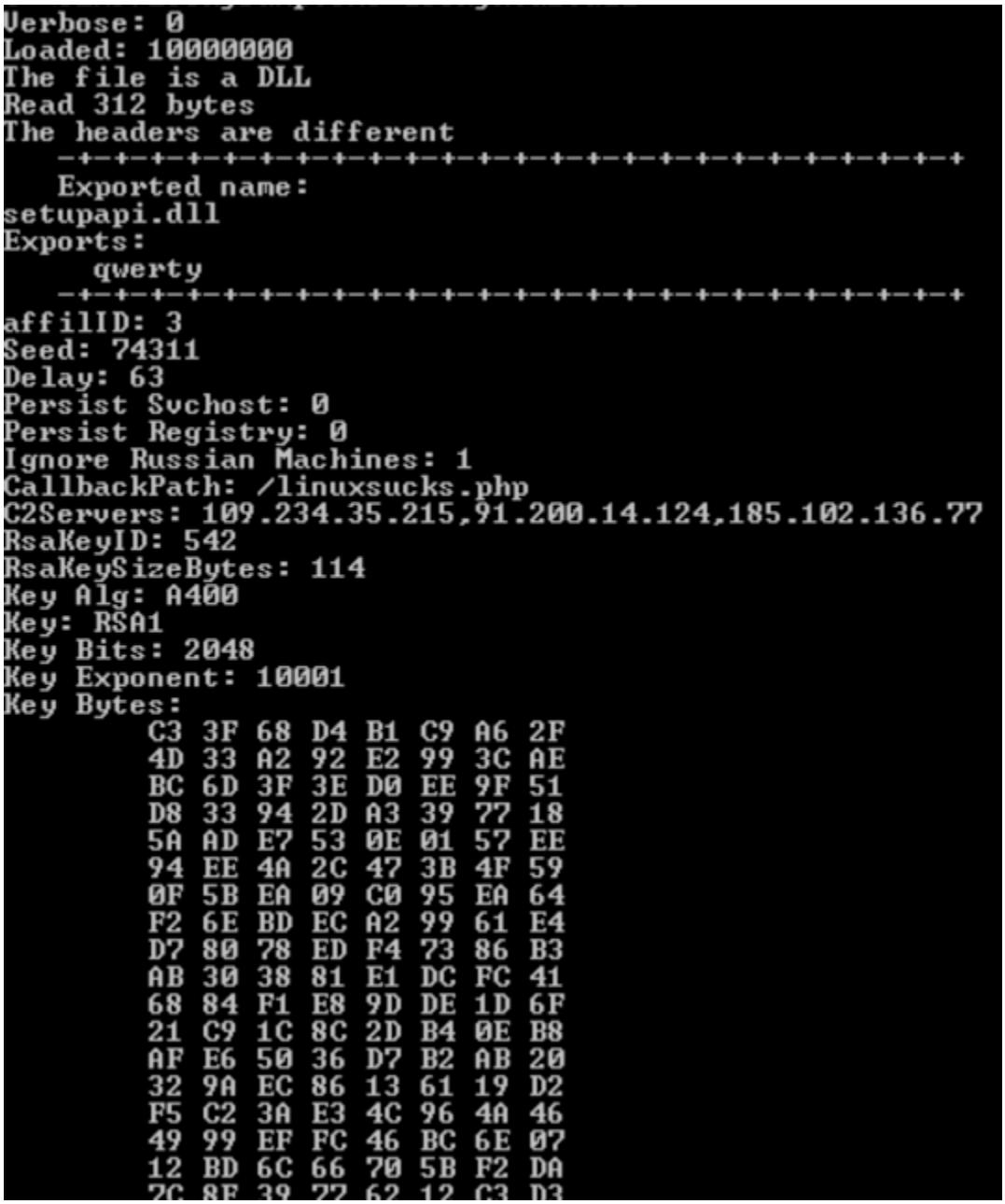


图 B：样本的 LockyDump 输出

Talos 总共研究了此垃圾邮件活动中的 13,384 封邮件。此活动包含 210 个独特样本（在下文可获取收录的样本）。

活动 2：“saved_letter_XXXXXXXX”垃圾邮件（联属 ID=1）

我们还研究了另一种散布 Locky 下载器的垃圾邮件活动，这种活动将 JavaScript (.JS) 文件用作下载勒索软件的机制。此活动的数量相对较少，其中的邮件使用“Complaint letter”作为主题来诱骗用户执行附加的文件。没人愿意收到投诉，因此很多收件人可能会迅速针对这些邮件采取行动。Talos 在 3 小时内研究了此垃圾邮件活动的 3,748 封邮件。这些邮件以

“Complaint letter”为主题，并且包含一个名为“saved_letter_XXXXXXXXX.zip”的 zip 附件，其中“X”代表 9 位十六进制字符。zip 附件中包含名为“saved letter XXXXXX.js”的 JS 恶意软件下载器，其中“X”代表 5-8 位十六进制字符。在这 3,748 封邮件中，我们发现了 388 个独特样本。

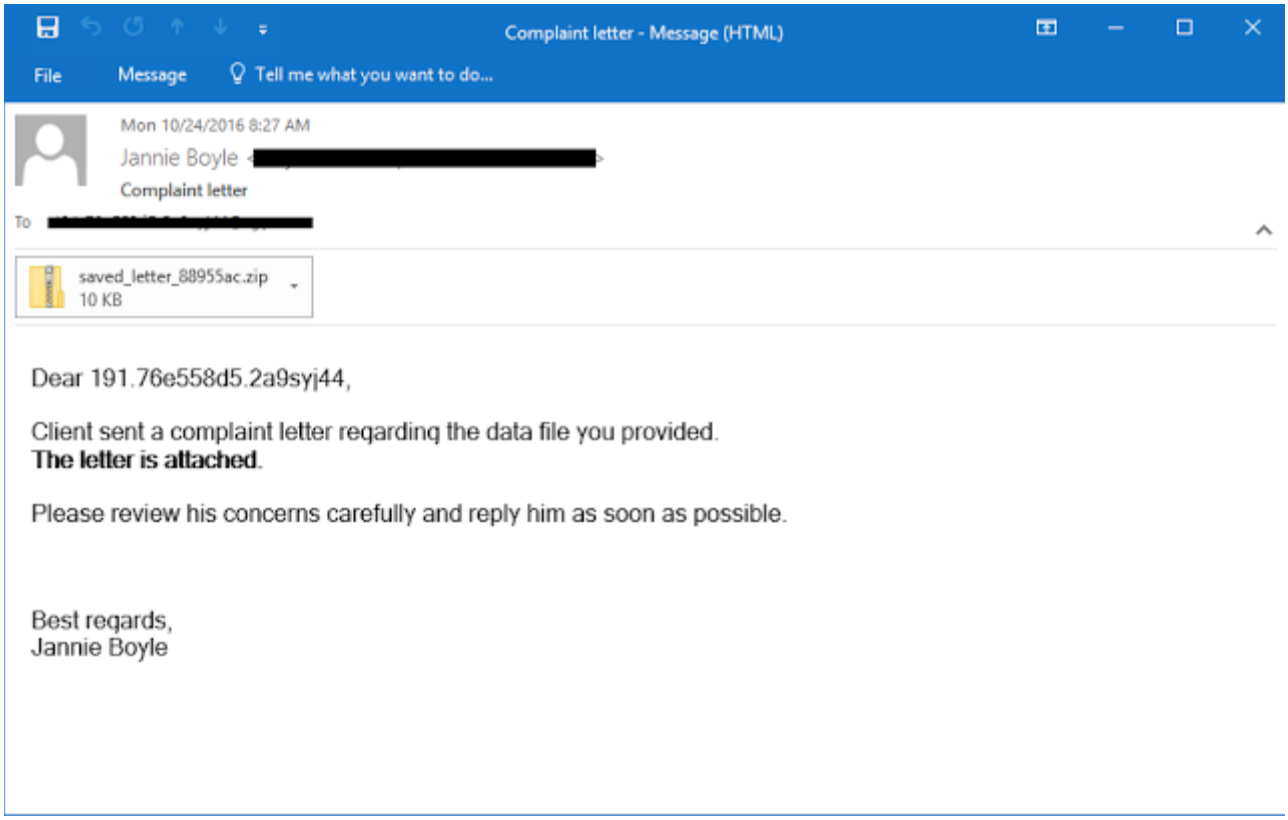


图 C：投诉邮件示例

活动 3：各种“Free”垃圾邮件（联属 ID=3）

除了前文介绍的两种活动之外，我们还研究了数量较少但形式多样的使用基于 WSF 的恶意软件下载器的垃圾邮件。这本身并非新创，自从在 2016 年 2 月出现以来，Locky 就频繁使用 JS 和 WSF 文件。有趣的现象是，在我们研究的与此活动关联的 154 封邮件中，有 133 封以法语用户为攻击对象，并且这些邮件将发件人伪装成法国电视和媒体运营商“Free”。此外，这些邮件声称是由“Free”发送的帐单。我们发现了 42 个与此活动关联的独特散列。邮件正文中称为收件人附上了金额为 XX.XX 欧元的帐单（在我们分析的所有邮件中，此金额均不相同）。

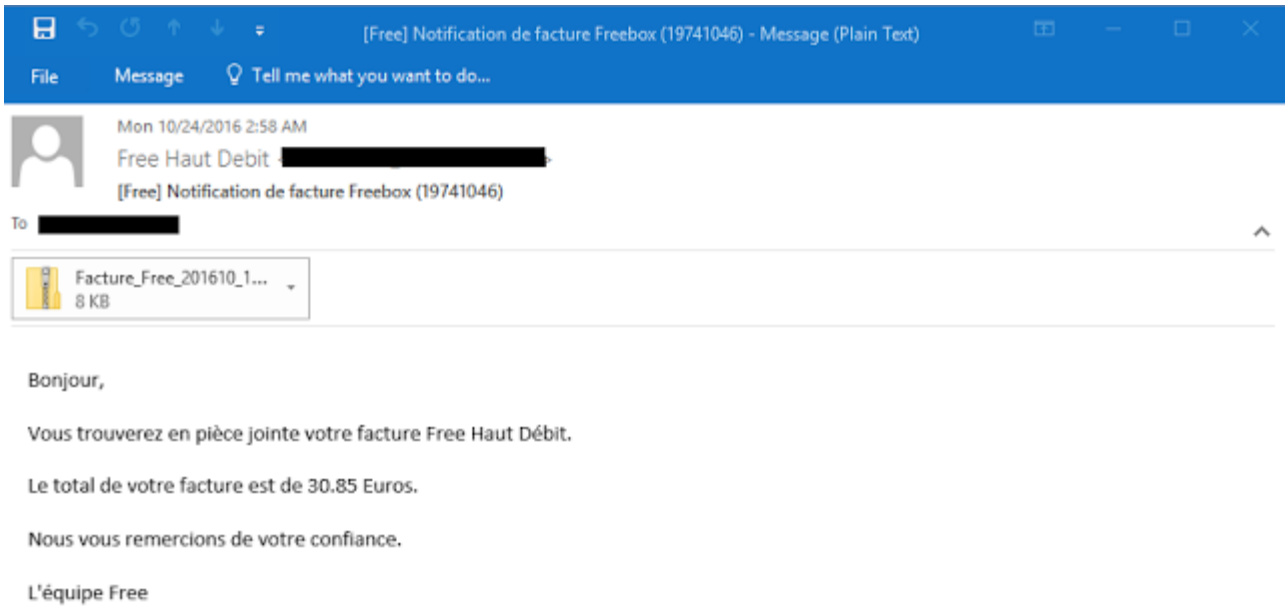


图 D：“Free”邮件示例

我们研究的剩余邮件都是各种与交付失败或通知请求相关的主题，例如：

主题：无法交付包裹，#000990048
主题：无法交付物品，#0000248834
主题：无法运送包裹，ID:00480186

这些邮件后面都采用使用 .ZIP 附件的 Locky 常规散布方法，.WSF 恶意软件下载器包含在附件中。我们相信，这第三种活动属于小规模测试活动，因为许多实例中出现附件损坏的情况。“Free”垃圾邮件以外的邮件均包含损坏的 .ZIP 附件，其中的文件使用“.doc.wsf”双扩展名，而且这些附件全部无效。垃圾邮件活动尝试用损坏比例如此之高的附件散布 Locky 下载器的情况非常罕见。

Locky 的变化

这些垃圾邮件活动散布的新版本 Locky 勒索软件在运作方式方面包含一些值得注意的变化。据我们研究，值得注意的变化包括：

- C2 使用的 URL 路径更改为 /linuxsucks.php。
- 加密文件所用的文件扩展名更改为“.shit”
- 包含勒索信的文件现在的文件名为“_WHAT_is.html”

危害表现

活动 1：

此处完整收录了此活动 210 个独特样本的散列

活动 2：

此处完整收录了此活动 388 个独特样本的散列

活动 3：

此处完整收录了此活动 42 个独特样本的散列

C2 域：

此处收录了我们研究的散布服务器的列表

防护

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	保护
AMP	✔
CWS	✔
ESA	✔
网络安全	✔
WSA	✔

高级恶意软件防护（AMP）解决方案可以有效防止执行威胁发起者使用的恶意软件。
CWS 或 WSA 的 Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。
IPS 和 NGFW 的网络安全防护功能拥有最新的签名库，可以检测威胁发起者的恶意网络活动。
ESA 可以拦截威胁发起者在攻击活动中发出的恶意电子邮件。

发布者：EDMUND BRUMAGHIN；发布时间：14:15
标签：LOCKY、恶意软件、勒索软件、垃圾邮件