

2016 年 6 月 30 日，星期四

立即行动，抵御猖狂的垃圾邮件攻击！

作者: [Warren Mercer](#)

摘要

据 Talos 观察，Zepto 勒索软件的活动有显著增长之势，并已确定，该恶意软件的一种传播方式是垃圾邮件。Locky/Zepeto 依然是目前最常见的勒索软件变体，有鉴于此，我们将重点关注这轮垃圾邮件攻击。在最近 4 天内，我们发现 137,731 封邮件使用了新的附件命名规范。此数字碰巧是回文式数字。这轮垃圾邮件攻击所使用的命名规范是“swift [XXX|XXXX].js”。其中，“swift”后面的“X”是某种字母/数字组合，我们发现这个组合既有 3 个字符组成的字符串，也有 4 个字符组成的字符串。此轮攻击开始于 6 月 27 日（星期一）。当天，我们的邮件安全设备（EAS）捕获了大约 4000 封邮件。在接下来的几天内，我们捕获的此类邮件数量不断上升，高峰期出现在随后的 4 天内的上午 7 点至 10 点和晚上 7 点至 10 点（UTC，即协调世界时）。

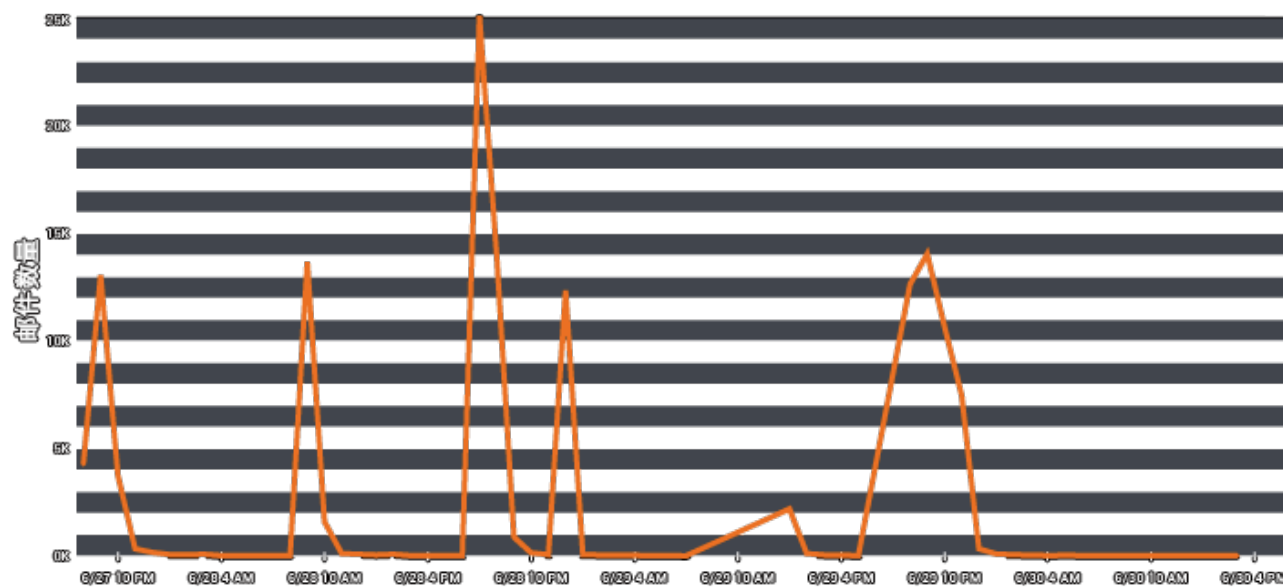


图 1. 邮件流量

我们检查了我们邮件遥测数据库中的 javascript 样本，从 13.7 万封邮件中确定了 3305 个唯一样本，其 sha256 散列见本文结尾。这些邮件都遵从“swift”命名规范，而且全部使用包含恶意 .js 的压缩 .zip 存档文件。它们尝试使用如下各种主题行欺骗用户，并冒用多种发件人身份（例如“CEO”或“销售部副总裁”）诱骗用户。

邮件正文内容通常是催促用户查看其“请求”的文档。邮件随附的 .zip 文件的名称一般由“收件人” 邮件地址信头加一下划线和一个随机数字组成：

Christopher Kelly @
To: recipient@example.com
Documents copies

Dear peter,

I am sending copies of the documents as attachments.

Thank you very much for your reply.

Regards
Christopher Kelly
"Divisional Managing Director"



pdf_copy-
peter_461397.zip

图 2. 邮件示例

邮件正文也经过定制，其中包含适于邮件群发功能的称呼语，例如“Dear”和“Hello”，再加上邮件地址用户名中的用户名字符串。在上面的示例中，称呼语部分显示的是“Dear Peter”。在这轮攻击中，随着时间的推移，邮件正文出现了一些细微的变化，主题信头也有所变化。我们观察到这轮攻击主要使用四种主题信头：

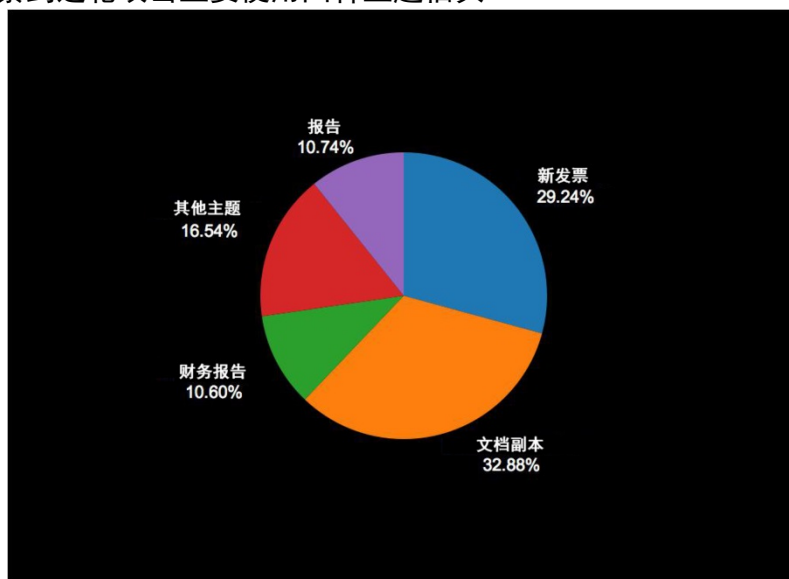


图 3.主题类别细分

当在沙盒中运行时，Zepto 会表现出很多可疑行为，使我们能快速确认其为恶意软件。

Analysis Report

ID	36d038b1d1326983a4aa203973d06fe2	Filename	swift 6d2.js
OS	2600.xpsp.080413-2111	Magic Type	JavaScript
Started	6/29/16 13:36:19	Analyzed As	js
Ended	6/29/16 13:42:10	SHA256	00e475ae83002930c6a9dd9c4223fd710c3a29a4c1c3775413d58e9e23e5c0b2
Duration	0:06:51	SHA1	79d7255b6fd0d5600d4d9c311d72003d308b4fda
Sandbox	phi-work-11 (pilot-d)	MD5	15ae1614b42526956a3855071553b056
		Tags	<input type="button" value="tag"/>

Behavioral Indicators

Threat Score: 95

Indicator	Severity	Confidence
Process Modified Desktop Wallpaper	100	95
A Script Established Direct IP Communications	90	90
Command Exe File Deletion Detected	75	100
Windows Picture And Fax Viewer Used To Display Decoy Image	70	100
Process Modified an Executable File	60	100
An HTTP Request Was Made to a Numeric IP Address	75	80
Process Created an Executable in a User Directory	60	95
Outbound HTTP GET Request	75	75
Process Modified File in a User Directory	70	80
Process Modified AUTOEXEC.BAT	80	70
A Script File Established Network Communications	70	80
Process Disabled Internet Explorer Proxy	70	70
Command Exe File Execution Detected	50	80
File Downloaded to Disk	30	90
Potential Code Injection Detected	50	50
DNS Response Contains Low Time to Live (TTL) Value	35	20
Outbound HTTP POST Communications	25	25
Outbound Communications to Nginx Web Server	25	25

图 4. ThreatGrid 行为

我们捕捉了一个有关正在运行的 Zepto 的视频，从中我们能看到此类恶意 JavaScript 代码的活动轨迹，以及它如何悄无声息地在受害者的电脑中使用 .zepto 扩展名缓慢地锁定文件：

视频 1. Zepto 感染

我们发现的 JavaScript 文件都包含“Swift”，且后面跟一个字符串。有趣的是，这个字符串由一个十六进制字符集（即 0 至 9 和 a 至 f）组成，我们尚不清楚其原因，但是这个有趣的观察结果非常值得注意。

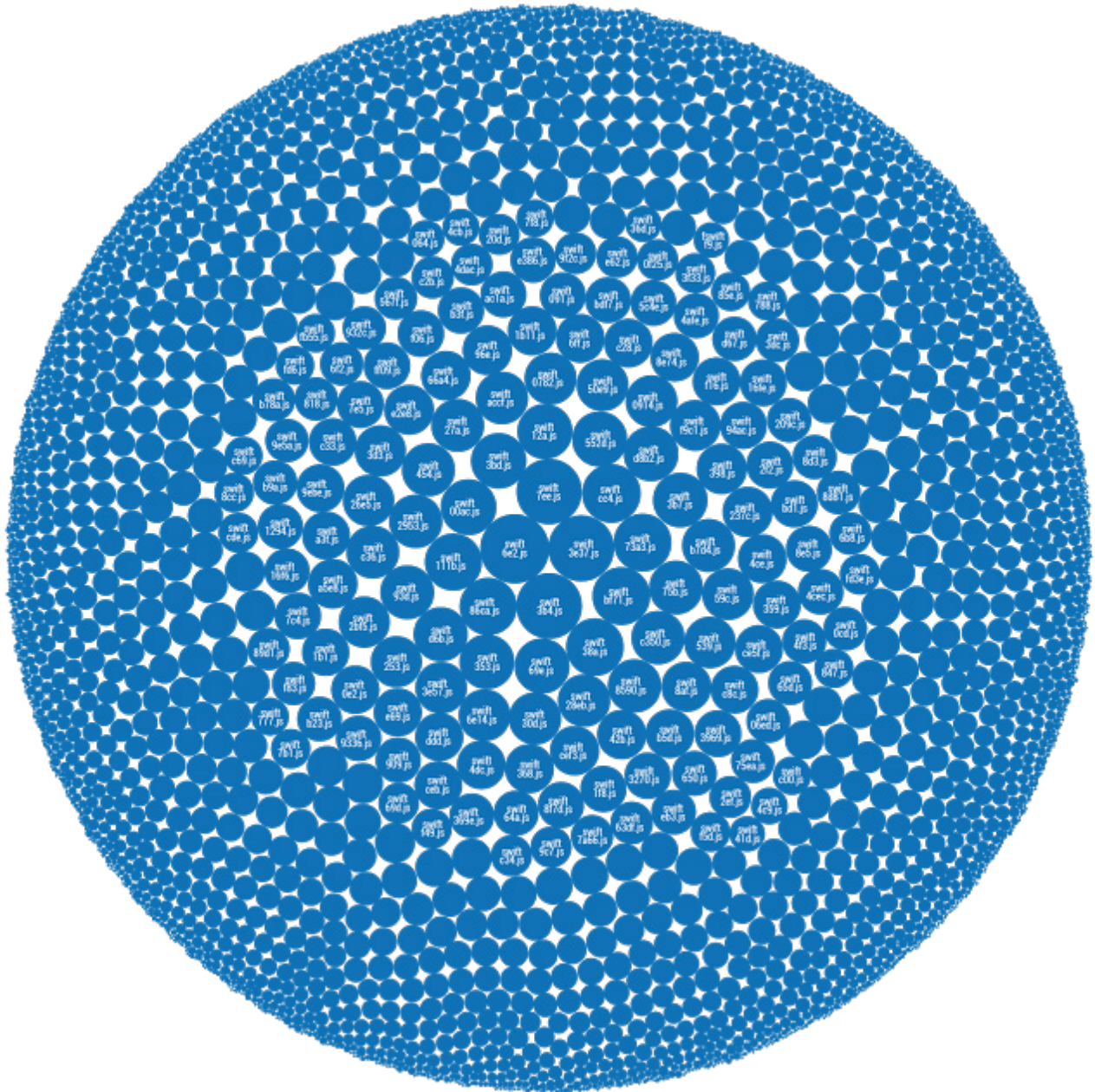
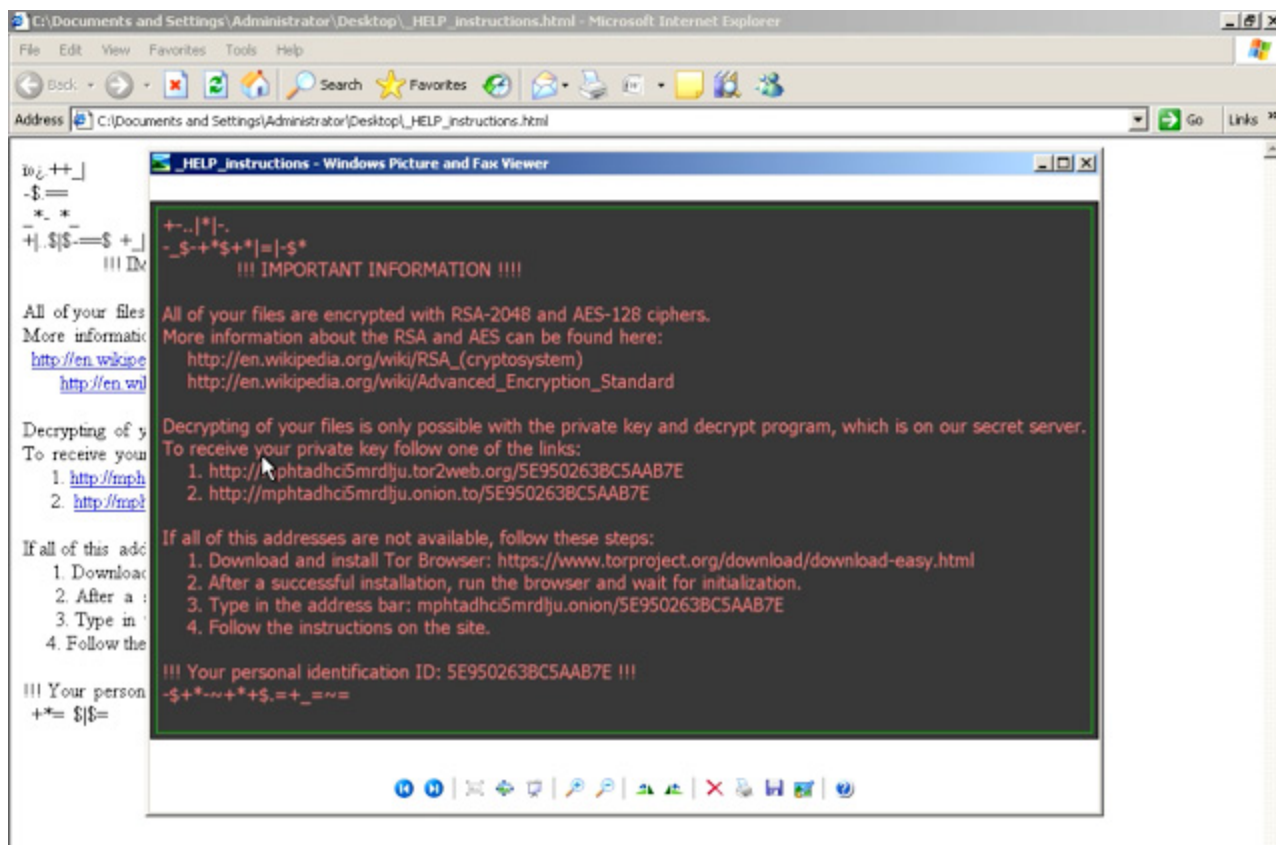


图 5.Swift 命名实例

这种恶意 JavaScript 执行后，会使用“wscript.exe”向定义的 C2 域发出 HTTP GET 请求。正是在这一步，不同样本之间会表现出差异，因为有些会向单个域发起连接，而另一些则最多能与 9 个域进行通信。

在下载并执行此二进制文件后，计算机将开始加密本地文件，然后向用户勒索赎金以解密文件。用户将会看到以下“_HELP_instructions”画面，这两个画面均来自 Internet Explorer，为恶意软件所放置的 HTML 文件，还有一个用 Windows Picture & Fax Viewer 显示的图片文件，计算机的背景/壁纸也会改变，以提醒您的计算机已被此恶意软件加密。



总结

这并不是一种新的攻击方式，但是它正在发展肆虐。如今的网络钓鱼/垃圾邮件攻击通常带有很大的相关勒索软件风险，这种攻击也不例外。现在人们所面对的攻击已能阻止用户访问文件，而且不幸的是，这种情况变得越来越普遍。网络攻击者根本不在乎对您造成了什么损害，或者他们勒索了什么，他们最后的目的就是赎金。电子邮件会继续被用作攻击媒介，因为现在人们的日常生活已离不开邮件，而且生成用于此类垃圾邮件攻击的大型邮件列表已变得越来越容易。由此类攻击活动导致的数据泄漏事件甚至包括向“竞标者”主动出售邮件数据。确保用户对邮件附件（例如此类攻击活动中使用的附件）保持警惕，有助于抵御这种攻击以及未来可能出现的其他垃圾邮件攻击。Talos 建议您务必制定一个妥善的备份策略，以防受到勒索软件攻击，而且我们强烈建议永远不要向这些攻击者支付赎金。

IOC

本文中提到的所有散列均在 [zepto_hash_IOCs.txt](#) 中列出。

防护产品

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邮件。

发布者：[WARREN MERCER](#)；发布时间：[19:10](#) 

标签：[恶意软件](#)、[勒索软件](#)、[ZEPTO](#)