THREAT INTELLIGENCE REPORT

PHISHING

THE SECRET OF ITS SUCCESS AND WHAT YOU CAN DO TO STOP IT

by Ray Pompon

F5 LABS

WHAT'S INSIDE

Introduction 2

How Phishers Bait Their Hooks with Information You Volunteer 3

How Attackers Collect Data About Your Employees 5

Social Media and Personal Information 6

Profiling 6

People Search Engines 8

How Attackers Gather Data about Your Organization 10

Your Organization's Internet Presence 12

Corporate Email Addresses 13

Beware of Data Leaking Out of Your Equipment 14

Application Platform Discovery 15

Email Headers 16

How Attackers Pull it all Together, and How You Can Fight Back 17

What Does a Phisher Need? 17

What to Do 18

INTRODUCTION

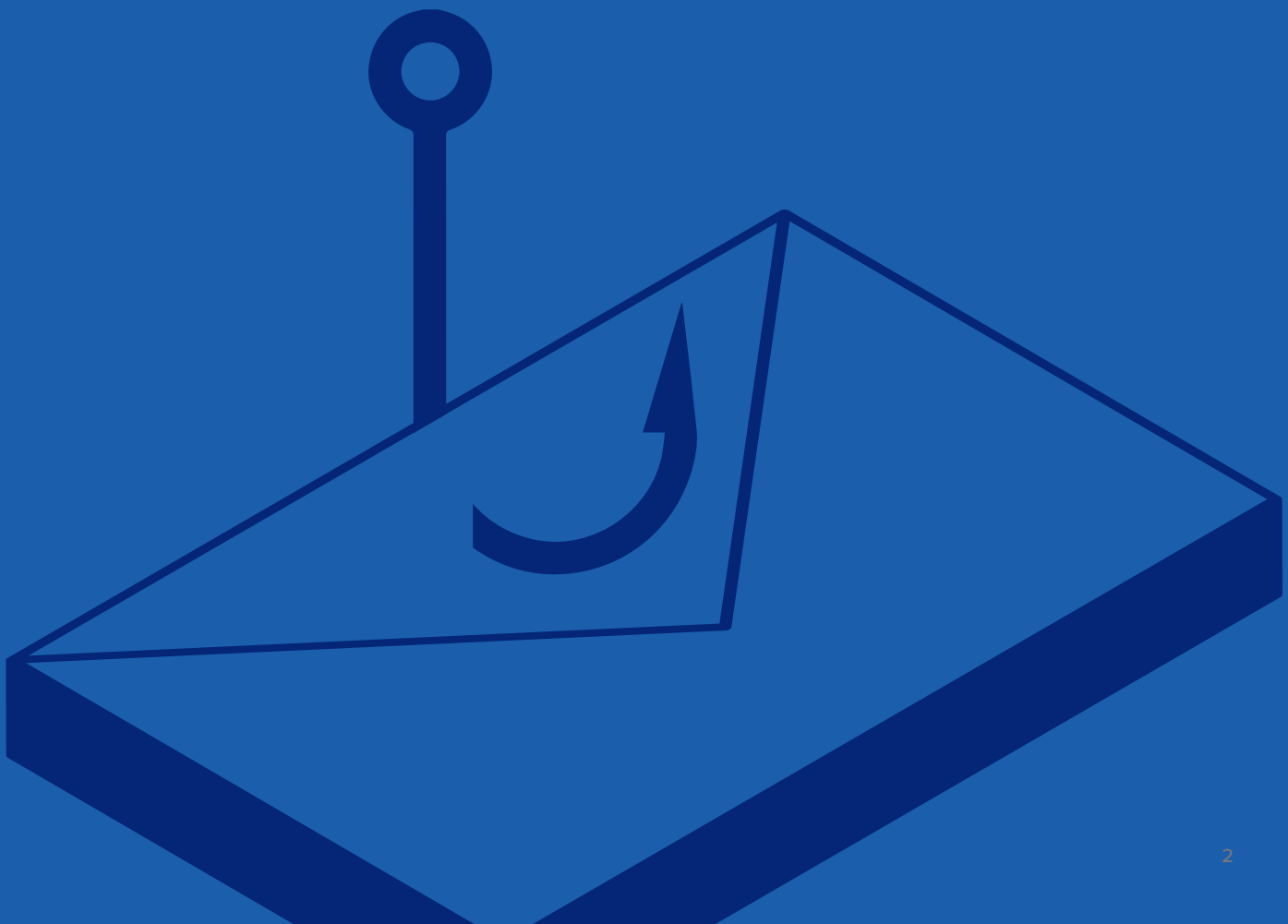
Phishing has proved so successful that it is now the number one attack vector.[1] The Anti-Phishing Working Group reports that in the first half of 2017 alone, more than 291,000 unique phishing websites were detected, over 592,000 unique phishing email campaigns were reported, and more than 108,000 domain names were used in attacks.[2] In 2016, the FBI's Internet Crime Complaint Center (IC3) received phishing reports from more than 19,000 victims.[3] However, IC3 also notes that only an estimated 15% of victims ever report crimes to law enforcement, so the actual total could exceed 125,000. Of the 19,000 reported cases, the total cost exceeded $31 million.

In this report, we explore why phishing campaigns work so well, how unsuspecting users play into the hands of attackers, and what organizations can do about it.

[1] https://www.csoonline.com/article/3036837/security/phishing-remains-top-attack-vector-for-criminals-both-novice-and-professional.html

[2] http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf

[3] https://pdf.ic3.gov/2016_IC3Report.pdf



HOW PHISHERS BAIT THEIR HOOKS WITH INFORMATION YOU VOLUNTEER

Seven minutes until his next meeting, Charles Clutterbuck, the CFO of Boring Aeroplanes, had just enough time to answer a few emails. He flopped onto his padded leather chair and tapped out his password. A dozen emails glowed unread at the top of his inbox stack. He skimmed down the list of names and subjects when one caught his eye. It was a from an old friend. With a nod, he clicked it up. "How's it going, Clutt?" the email began. He smiled at the old nickname from the dorm days when he first met Bill. Funny that Bill was emailing him at his work address, but that question was quickly forgotten as he skimmed the message.

From: Bill Fescue b.fescue@blafmail.com
Sent: Thursday, July 6, 2017 12:16
To: Charles Clutterbuck c.clutterbuck@boringaeroplanes.com
Subject: My new hoss

How's it going, Clutt?

Hit the track with my new Falkens and, guess what? Tremendous grip! No more wheel spins. Check out my track time and cornering: http://vizodsite.com/istruper_video_10

See you at next week's Autocross?

~Bill

As you might have guessed, this is a spear phishing email.

In spear phishing, the attacker leverages gathered information to create a specific request to trick someone into running something or giving up personal information. It's an extremely successful technique and attackers know this. In fact, the Anti-Phishing Working Group reports that phishing has gone up 5,753% over the past 12 years.[4]

[4] http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf

Phishers work by impersonating someone trusted by the target, which requires crafting a message that is credible and easily acceptable. To do this, the phisher needs information about the target to construct their disguise and bait the hook. They get this information by research and reconnaissance.

In the example above, an executive at a military plane parts supplier received an email apparently from a friend. His interest in car racing—as well as his friend's name and style of speaking—was plucked off social media. The attacker spent a few minutes of web research on car racing to get the vernacular right

and then created an email account in the friend's name. The link is to a site with a video server that sends an exploit geared to the target's laptop operating system (gleaned from research on the company infrastructure). It loads specialized malware built to exfiltrate aerospace intellectual property. Easy, peasy.

So, we know that attackers are gathering information from social networks and various Internet sources, but just how much information is available? Defenders spend quite a bit of energy preventing the obvious information leaks like passwords, crypto keys, and personally identifiable information (PII). Those are high impact information leaks, but what about the low impact ones?

It's worth exploring what's typically discovered in an attacker's passive electronic reconnaissance. And, that's not counting active recon like calling the company's main phone number and trying to extract information via pretexting[5] or going onsite for dumpster diving.[6] This is all low-risk stuff that can happen in secret from afar. But, as the Great Detective said, "You know my method. It is founded upon the observation of trifles."[7]

[5] http://www.scambusters.org/pretexting.html

[6] https://www.social-engineer.org/framework/information-gathering/dumpster-diving/

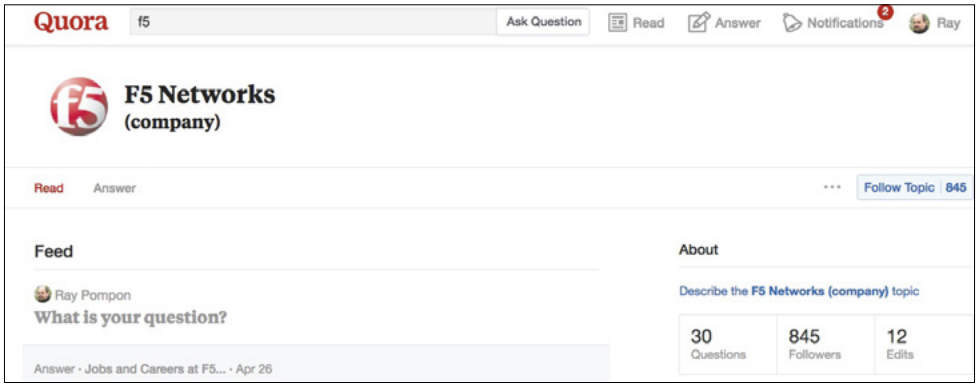
[7] https://en.wikiquote.org/wiki/Sherlock_Holmes

HOW ATTACKERS COLLECT DATA ABOUT YOUR EMPLOYEES

We've seen an everyday example of how easily a competent corporate executive (or any other employee, for that matter) can be drawn into a phishing scam through social engineering. Now let's look at how some of the seemingly innocent actions we take (information we post) on the Internet make the job of a phisher simple—like taking candy from a baby.

Since spear phishers go after a specific organization, they need to know who works there before they can begin their targeting. A lot of people tag themselves on various social media sites as an employee of a particular company. LinkedIn is a site that provides lots of details on where people work. Quora is another site where tech people congregate:

FIGURE 1



Through these sites, it's not hard for phishers to gather up a list of names of employees at a specific organization.

SOCIAL MEDIA AND PERSONAL INFORMATION

Despite the security team's best efforts to prevent it, employees will share and spread information about themselves all over the Internet. Social media companies expend tremendous effort to encourage people to join and post information about themselves. Some valuable bits of information that attackers can use are:

- **Work history**
- **Education information (college and high school attended)**
- **Family and relationship information**
- **Comments on links**
- **Dates of important life events**
- **Places visited**
- **Favorite sites, movies, TV shows, books, quotes, etc.**
- **Photographs**

PROFILING

All these pieces of information provide powerful leverage points for attackers, but they also provide a lot of valuable indirect information. As our phishing example above points out, attackers can observe the writing style of the people they want to impersonate. Beyond that, they can also create detailed psychological profiles of victims. There are a number of tools and techniques available to do things like:

- **Analyze sentiment to determine people's opinions and political leanings**[8]
- **Analyze posting times to determine when people are awake (and asleep) and what their home time zones are**[9]
- **Determine an individual's personality type, which can inform manipulation techniques**[10]
- **Analyze relationships and friendship ties**[11]

[8] https://scholar.google.com/scholar?hl=en&q=Sentiment+analysis+of+social+media+&btnG=&as_sdt=1%2C45&as_sdtp=

[9] http://www.automatingosint.com/blog/2016/03/osint-facebook-when-people-sleep/

[10] https://www.onlineprivacyfoundation.org/opf-research/big-5-experiment-arch/

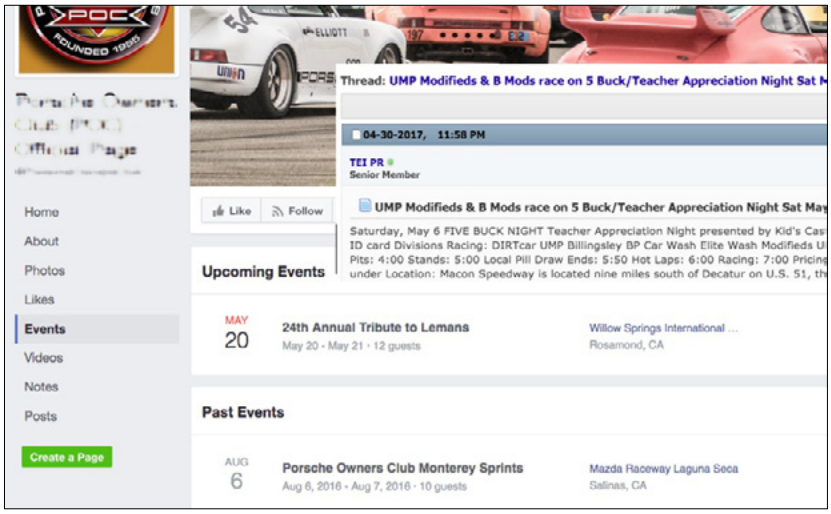
[11] http://www.pcworld.com/article/2056080/facebook-stalker-tool-uses-graph-search-for-powerful-data-mining.html

With sites like Facebook that host nearly 2 billion users,[12] it's very easy to craft a Google search for someone with "[name] [location] site:facebook.com" to find their page.

[12] http://money.cnn.com/2017/02/01/technology/facebook-earnings/

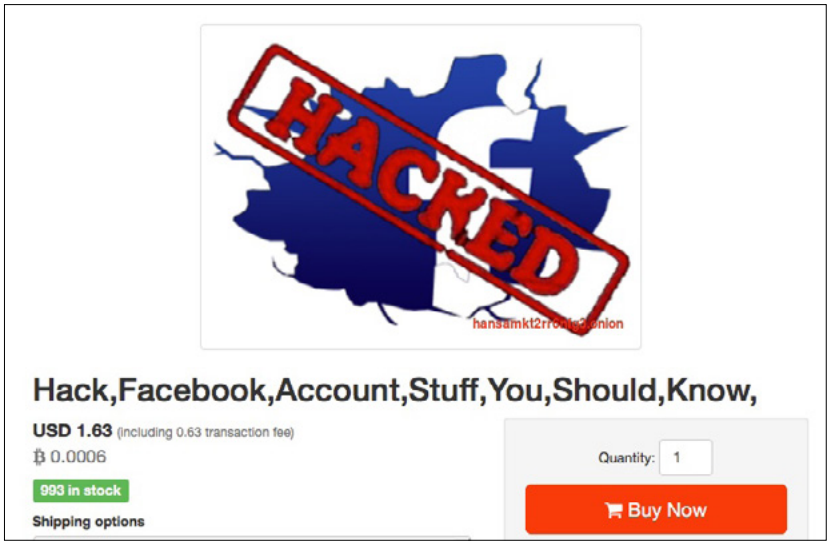
Many social media users are part of interest groups, which can provide useful leverage points for a phisher.

FIGURE 2



Even when someone sets their social media profile to "private," it's still not too difficult for an attacker to break in and get what they want. Here is a hacking service being advertised on a Darknet for just that purpose:

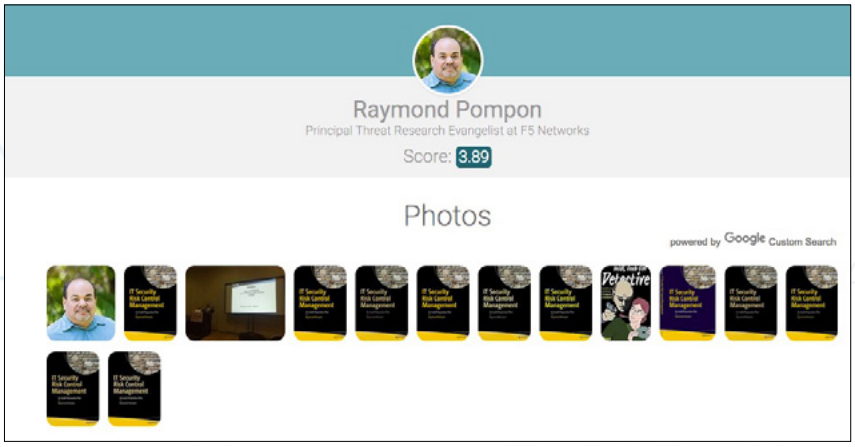
FIGURE 3



PEOPLE SEARCH ENGINES

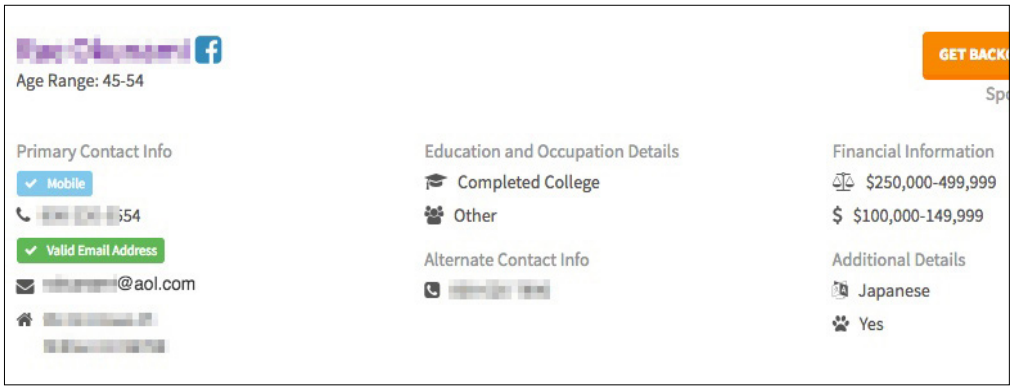
In addition to social media sites, there are numerous "people search" sites like Pipl, Spokeo, and ZabaSearch. Many of these sites pull together profiles based on dozens of resources. Sometimes they're not very helpful, like this example for me, because I'm a paranoid security guy:

FIGURE 4



However, different sites can dig up some interesting data, like this example:

FIGURE 5



Note how this site provides Facebook information, email address, annual income, education, phone number, age range, and even racial profiling. Here's some typical information you can get from these kinds of sites:

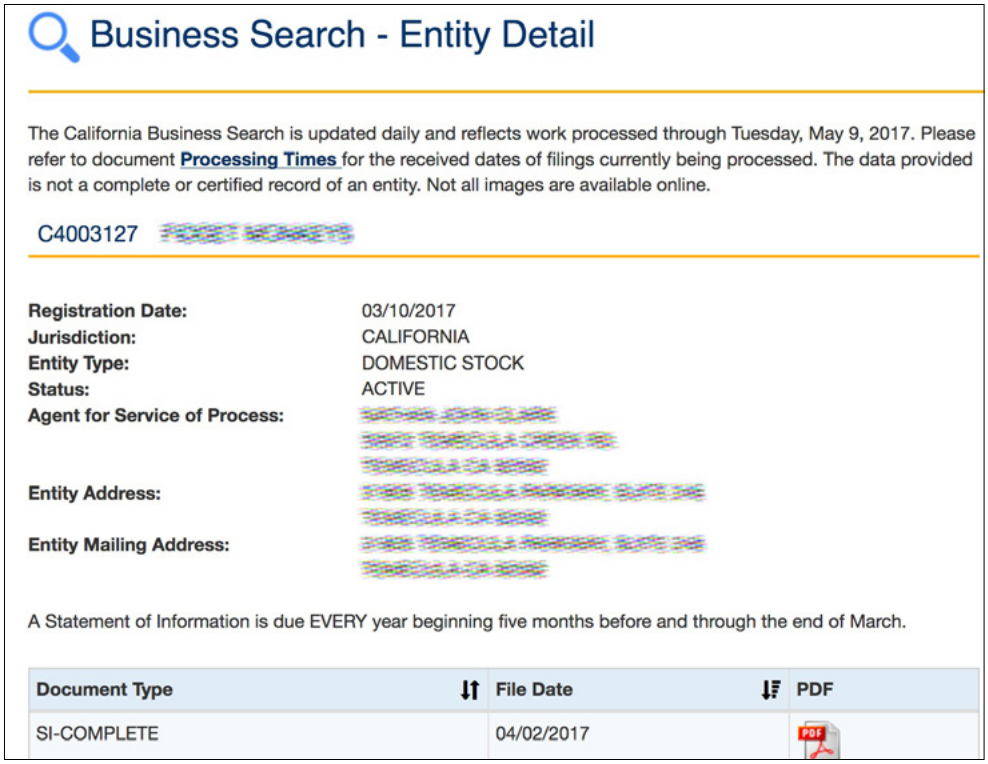
- **Home address**
- **Mobile phone number**
- **Home (landline) phone number**
- **Age**
- **Salary range**
- **Spouse and family**
- **Email address, which leads to possible usernames**
- **Middle name**
- **Maiden name**

Most employees don't think about things like this—because most employees don't think like bad guys. It doesn't occur to them how much personal and work-related information they are freely volunteering on various websites—or how easy they make it for phishers to pull information together into some pretty comprehensive professional dossiers. The lesson here is think before you volunteer information about yourself and your work, and limit the number of websites where you do this.

HOW ATTACKERS GATHER DATA ABOUT YOUR ORGANIZATION

When attackers want to go after a specific organization but need to know which individuals within that organization to target, then they need to dig through corporate and business records. They can start simply with the ownership records, which are freely available over the web, as in this example:

FIGURE 6



Business Search - Entity Detail

The California Business Search is updated daily and reflects work processed through Tuesday, May 9, 2017. Please refer to document **Processing Times** for the received dates of filings currently being processed. The data provided is not a complete or certified record of an entity. Not all images are available online.

C4003127 [redacted]

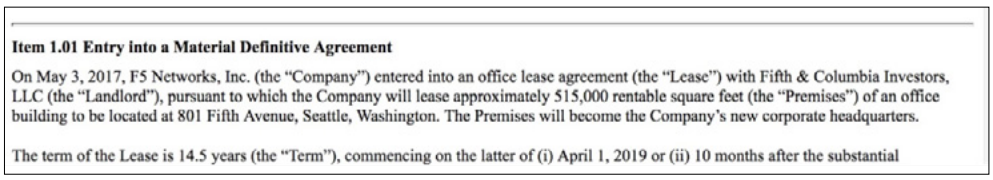
Registration Date:	03/10/2017
Jurisdiction:	CALIFORNIA
Entity Type:	DOMESTIC STOCK
Status:	ACTIVE
Agent for Service of Process:	[redacted]
Entity Address:	[redacted]
Entity Mailing Address:	[redacted]

A Statement of Information is due EVERY year beginning five months before and through the end of March.

Document Type	File Date	PDF
SI-COMPLETE	04/02/2017	

Publicly traded companies have even more information available online from their SEC filings. Here is an excerpt from a recent 8-K filing from F5 about our new corporate headquarters:

FIGURE 7



Item 1.01 Entry into a Material Definitive Agreement

On May 3, 2017, F5 Networks, Inc. (the "Company") entered into an office lease agreement (the "Lease") with Fifth & Columbia Investors, LLC (the "Landlord"), pursuant to which the Company will lease approximately 515,000 rentable square feet (the "Premises") of an office building to be located at 801 Fifth Avenue, Seattle, Washington. The Premises will become the Company's new corporate headquarters.

The term of the Lease is 14.5 years (the "Term"), commencing on the latter of (i) April 1, 2019 or (ii) 10 months after the substantial

Many corporations that have been around for more than a few years have probably been involved in a lawsuit or three. Attackers can pull those records, as well, like this example from now defunct Eastern Airlines:

FIGURE 8

	Party Name	Court	Case	NOS	Date Filed
1	Eastern Airlines (dft)	flsdce	1:1984-cv-01700	310	07/17/1984
2	Eastern Airlines (dft)	nyedce	1:1992-cv-05927	310	12/16/1992
3	Eastern Airlines Benefit Retirement Income Plan For Pilots, (dft)	flsdce	1:1990-cv-01113	791	05/09/1990
4	Eastern Airlines Inc (dft)	wawdce	2:1987-cv-00815	310	06/10/1987
5	Eastern Airlines Inc., (dft)	flsdce	1:1983-cv-03017	310	12/09/1983
6	Eastern Airlines Inc., (pla)	flsdce	1:1988-cv-00804	470	05/06/1988
7	Eastern Airlines, Inc (dft)	flsdce	1:1987-cv-01272	740	07/06/1987
8	EASTERN AIRLINES, INC. (pla)	dcdce	1:1990-cv-02879	890	11/21/1990
9	Eastern Airlines (dft)	flsdce	1:1984-cv-01703	310	07/17/1984
10	Eastern Airlines (dft)	nyedce	9:1990-cv-04416	310	12/21/1990
11	Eastern Airlines Employee Welfare Benefit Plan (dft)	madce	1:1993-mc-10265	0	04/07/1993
12	Eastern Airlines Inc. (dft)	nyedce	1:1987-cv-04254	310	12/21/1987
13	Eastern Airlines Inc., (dft)	flsdce	1:1983-cv-03079	310	12/15/1983
14	Eastern Airlines Inc., (pla)	flsdce	1:1989-cv-00447	740	03/03/1989
15	Eastern Airlines, Inc (dft)	mddce	1:1986-cv-02906	350	09/19/1986
16	EASTERN AIRLINES, INC. (pla)	dcdce	1:1989-cv-03473	890	12/29/1989
17	Eastern Airlines (dft)	flsdce	1:1984-cv-00922	310	04/12/1984
18	Eastern Airlines (res)	nmdce	1:1990-cv-01171	380	12/13/1990
19	EASTERN AIRLINES (dft)	pawdce	2:1987-cv-00908		04/29/1987

Like the people search databases, there are also aggregator search tools for corporations, such as OpenCorporates, that pull together a lot of this information into a single place.

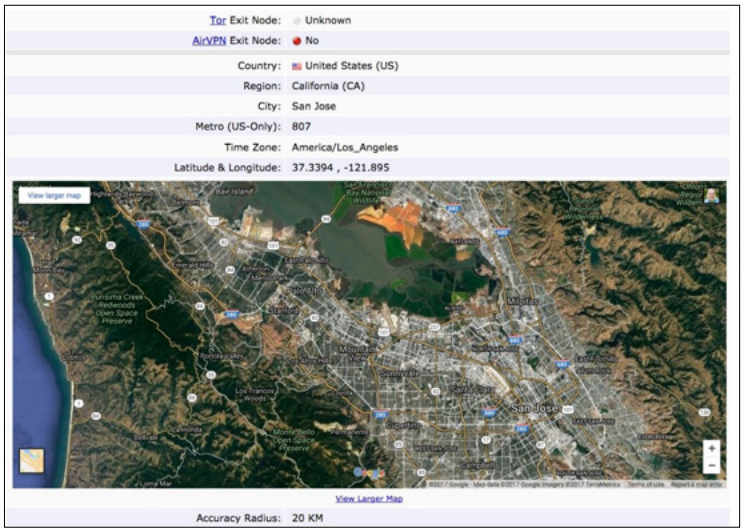
FIGURE 9

These sources can help attackers build profiles of individuals and department names, which are powerful tools for flavoring their phishing bait. Scanning a company's website can also give you clues about business partners and affiliates, for which you can repeat all of these searches.

YOUR ORGANIZATION'S INTERNET PRESENCE

Everyone active on the Internet has an IP address, and IP addresses can provide some basic information about where they terminate and who owns them.

FIGURE 10



Granted, some of this information can be misleading because IP addresses can trace back to the ISP rather than the actual organization. But, sometimes attackers get lucky. Most of the time, they can uncover where sites are being hosted and gain some basic information about the company's network configuration.

In addition to the IP address information, every organization with a domain has domain registration information. Like IP information, for most sizable organizations, it's going be generic and not reveal much that's useful. But again, sometimes attackers get lucky.

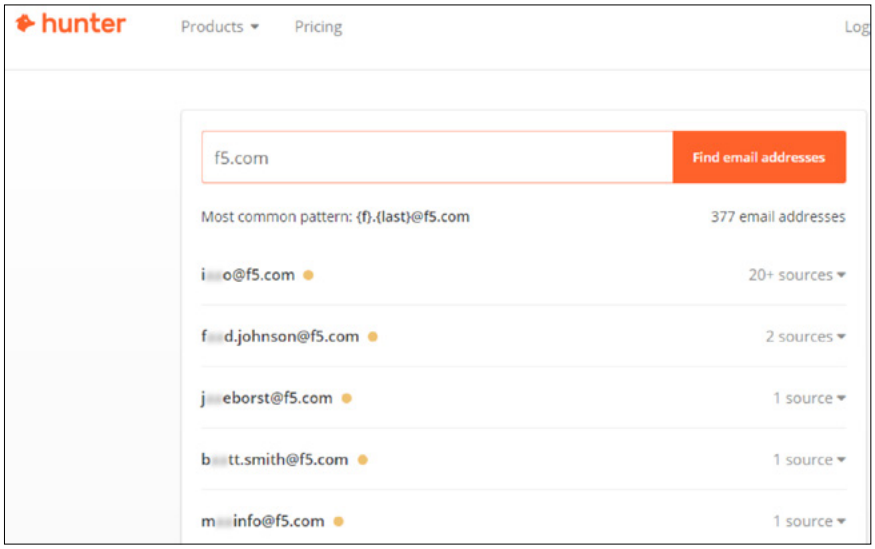
FIGURE 11

CORPORATE EMAIL ADDRESSES

Where else can attackers find usable email addresses for an organization? There are many companies out there that can help with that. Here's Hunter,[13] which not only provides email addresses but also provides hints on the email format used.

[13] https://hunter.io/

FIGURE 12



BEWARE OF DATA LEAKING OUT OF YOUR EQUIPMENT

To pull off successful phishing scams, at a minimum, attackers need information about your organization and your employees. We've already seen several ways they go about getting this information. But one area organizations often overlook is the information that's leaking out of their systems.

Improperly configured network systems and applications can leak internal configuration and infrastructure information. This can include information like server names, private network addresses, email addresses, and even usernames. Devices and software that have been known in the past to leak internal data onto the Internet include DNS servers, self-signed certificates, email headers, web servers,[14] web cookies, and web applications.[15]

Here is a simple example of how a sloppily configured web server can reveal the internal IP addressing scheme:

```
HTTP/1.0 200 OK
Date: Mon May 22 15:31:46 PDT 2017
Server: Macrohard-YYZ/6.0
Connection: Keep-Alive
Content-Type: text/html
X-Powered-By: BTQ.NET
Accept-Range: bytes
Last-Modified: Sat, May 20 04:14:01 PDT 2017
Content-Length: 1433
Connection-Location: http://192.168.0.10/index.htm
```

Attackers can also comb through web application source code to look for developer names, internal code words, and even references to supposedly hidden services.[16] Almost all of these kinds of technical information leakages are rated very low impact and are usually deprioritized in remediation.

[14] https://support.microsoft.com/en-us/help/967342/fix-the-internal-ip-address-of-an-iis-7.0-server-is-revealed-if-an-http-request-that-does-not-have-a-host-header-or-has-a-null-host-header-is-sent-to-the-server

[15] https://www.owasp.org/index.php/Top_10_2007-Information_Leakage_and_Improper_Error_Handling

[16] https://www.owasp.org/index.php/Review_webpage_comments_and_metadata_for_information_leakage_(OTG-INFO-005)

APPLICATION PLATFORM DISCOVERY

Applications are rarely built from scratch but are instead assembled from libraries and existing frameworks. All of these application components can contain vulnerabilities as well as clues to the development team and processes in an organization. There are numerous easy-to-use tools that can uncover what is being deployed. Here is the BuiltWith tool's analysis of a site:

FIGURE 13

EMAIL HEADERS

An excellent source of internal configuration information can be gleaned from email headers. Attackers can simply fire off a few email inquiries to folks at an organization and see what they can find. Here's a typical email header using our example company, Boring Aeroplanes. Note both internal and external IP addresses are shown, along with server names:

Received: from edgeri.boringaeroplanes.com (host-12-154-167-196.boringaeroplanes.com. [**312.154.167.296**])
Received-SPF: pass (google.com: domain of charles.clutterbuck@boringaeroplanes.com designates **312.154.167.296** as permitted sender) client-ip=**312.154.167.296**;
Received: from edgeri.boringaeroplanes.com (172.31.1.48) by **WEXCRIB00001059.corp.internal.boringaeroplanes.com** (**172.31.1.42**) with **Microsoft SMTP Server** id 14.3.301.0; Fri, 28 Apr 2017 10:40:36 -0400
Received: from **WEXCRIB00001065.corp.internal.boringaeroplanes.com** (**70.338.297.31**) by WEXCRIB00001059.corp.internal.boringaeroplanes.com (172.31.1.42) with Microsoft SMTP Server (TLS) id 14.3.301.0; Fri, 28 Apr 2017 10:39:23 -0400
Received: from WEXCRIB00001054.corp.internal.boringaeroplanes.com ([**169.254.9.522**]) by WEXCRIB00001065.corp.internal.boringaeroplanes.com ([70.338.297.31]) with mapi id 14.03.0301.000; Fri, 28 Apr 2017 10:39:31 -0400
From: "Clutterbuck, Chuck" <charles.clutterbuck@boringaeroplanes.com>
Subject: Inquiry
Thread-Topic: Inquiry
Thread-Index: AdLAKumC2+2KaqenReOr0muBBLJpfQ==
Date: Fri, 28 Apr 2017 14:39:30 +0000
Accept-Language: en-US
x-originating-ip: [**10.16.15.170**]
x-keywords4: SentInternet
x-cfgdisclaimer: Processed
MIME-Version: 1.0
Return-Path: charles.clutterbuck@boringaeroplanes.com

From this, attackers have a number of IP addresses, and they know what software the mail server is running and how email flows out of the organization.

HOW ATTACKERS PULL IT ALL TOGETHER, AND HOW YOU CAN FIGHT BACK

By now, it should be pretty evident why phishing scams are becoming so rampant. Information about individuals and corporations is readily available and easy to find on the Internet, making it easy for attackers to pull phishing schemes together—and with great success.

None of the bits of information we discussed above is particularly dangerous by itself, so most people are not concerned. However, one of the principal tenets of information theory is that each piece of information becomes more valuable as you find more related pieces of information. One bit of low impact information is slightly useful. Two bits of related information makes both more useful. Add three, five, or ten pieces and the value can become inestimable.

WHAT DOES A PHISHER NEED?

Let's walk through how an attacker can use specific information about individuals and corporations to build a phishing scam. Their first, key objective is to zero in on the correct person within the organization to accept the phishing "hook." This means finding the names of persons through organizational data research. The attacker's goal is to identify the people in key positions who have access to the data to be hacked. Barring that, attackers try to find the people who know the people in key positions so they can work their way through the inside network toward the goal. If that doesn't work, an attacker can also go after individuals at trusted partner or supplier companies, leveraging their relationships and access to find a way in.

Once an attacker identifies the specific individuals, they can psychologically profile them based on their social media postings and affiliations. (In some cases, instead of phishing, an attacker might look for websites that the victim frequents and compromise those sites to plant drive-by downloads.[17] This is called a Watering Hole Attack.[18])

For crafting a phishing email, an attacker can use all the social media postings and organizational information to create the lure. They can go directly at an individual's interests and friends, like in the example given above. They can also go indirectly and use organizational information and spoof the company's HR department to ask employees to verify basic information.[19] Knowing which individuals to impersonate in HR can help solidify the phishing email.

[17] https://en.wikipedia.org/wiki/Drive-by_download

[18] https://en.wikipedia.org/wiki/Watering_hole_attack

[19] https://security.berkeley.edu/news/phishing-example-message-human-resources

The attack doesn't end there. The cyber crook wants to break into the network and probably plant malware to steal data. To make sure the malware works properly, they customize it for the appropriate versions of software running internally and the IP networks in use. In the example used above, the attacker sent an exploit specifically tailored for the version of software running on the victim's machine. Sneaking stolen data back out, called exfiltration, is always a challenge, but knowing what internal servers there are and where they're located can provide an easy roadmap.

WHAT TO DO

There's a limit to what we as security professionals can do to keep people from sharing information on social media. In government agencies, there are more restrictions and education around this kind of behavior (called operational security[20]). In the private and commercial world, corralling such behavior is much harder. So, security awareness training, citing these examples, is a good place to start. At least users will be aware of the consequences of their sharing and be forewarned to the deviousness of the attacks. Users should also be urged to report any suspicious emails and verify with IT or Security before running outside software or providing their login credentials.

A good resource you can offer your users is this advice from Public Intelligence on how to reduce their online exposure by "opting out."[21] The fewer bits of data attackers can latch onto, the better.

It is a good idea for your security team (or better yet, your threat intelligence team) to periodically scan your own organization or hire a penetration tester. This could give you clues as to who and where attackers will strike first.

Closing the information leakage on your Internet-facing gear is often not hard to do and is recommended. Every door you close denies an attacker another puzzle piece of information. All domain and IP registries should be set up with generic role names and identifiers instead of the names of individuals. Most IT folks do this anyway to reduce potential spam, but it doesn't hurt to check.

Lastly, contracting with a good penetration testing firm to do reconnaissance and a social engineering test is a great way to see what you might have missed. It's better to pay and control the results of a mock attack than have to live through a real one.

[20] https://en.wikipedia.org/wiki/Operations_security

[21] https://publicintelligence.net/njroic-opting-out/

APPLICATION THREAT INTELLIGENCE

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com