

A blurred, high-angle shot of a modern office hallway. Several people are walking in different directions, their figures motion-blurred to convey a sense of activity and movement. The hallway has large windows on the right side, letting in bright light. The floor is polished and reflective.

proofpoint®

Ransomware and Cloud Risk Exposures

Chris Richmond

Solutions Engineering Leader East and Canada

crichmond@Proofpoint.com


917-617-0361


What is the Ransomware Landscape?


What is Ransomware?

- Ransomware is typically a low end malware
- It is typically part of a larger attack infection chain
 - Key is to block the initial loading agent from entering into the environment
- Purpose is to lock system access to critical files by encrypting the data
- Tends to spread as a worm after initial infection causing greater risk to organizations
- Ransomware has historically been associated to Nation State attackers
 - Motivations: Funding, Incident Response monitoring, Infrastructure Damage
- Sharp decline over the last 2 yrs but in past 8 months on a major upswing
- Examples: GandCrab and Sodinoknobi (email) Ryuk and SamSam (not mail) but in many cases the entry compromise was mail

Hacking is a Business

edbitss 
Vendor Of DiamondFox



Posts: 39
Joined: Apr 2016
Reputation: 
Jabber: edbitss@blah.im

Hello guys, im really happy to start a sales thread of the new DiamondFox version: Post: #1

Panel:
Spoiler [\(Click to View\)](#)

Builder:
Spoiler [\(Click to View\)](#)

*Some information was blurred cause this address still in use for a campaign.

Loader:

- Core totally recoded.
- Stability Improved.
- size Improved (18kb with configurations).
- No dependencies.
- Full windows compatibility (x86 and x64 from XP to Windows 10).
- New cryptographic methods.
- New installation routines (Bypass AVs proactives).
- Domain generation algorithm support.

Panel:

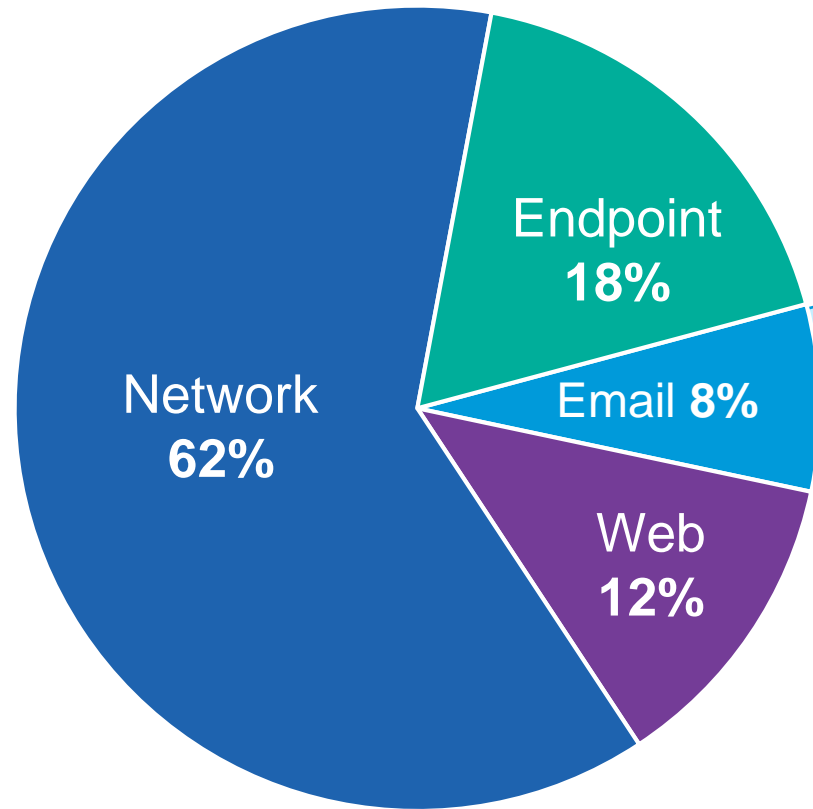
- Fully realtime (AJAX/JS) showing the last action/report sent or received for the bot.
- Extra security added: antforce, captcha and ban suspicious queries.
- The web panel can be hosted on windows servers without any kind of error.
- All communication with the panel are encrypted with a custom algorithm.

Plugins:

- Browsers Password Stealer (Internet Explorer, Mozilla Firefox, Google Chrome, Yandex Browser, Opera).
- FTP Stealer (Filezilla).
- DDoS (UDP, Layer7 [3 Methods], HTTP).
- Keylogger (Keyboard Hook, HTML Report, Clipboard Watcher, Get Window Title, Get Time, Can be triggered by window).
- Email grabber (Outlook Express, Microsoft Outlook 2000 [POP3 and SMTP], Microsoft Outlook 2002 to 2016, Windows Mail, Windows Live Mail, IncrediMail, Eudora, Netscape, Thunderbird, Yahoo! Mail, Hotmail/MSN mail, Gmail).
- RDP/VNC recover (Windows RDP, TightVNC, UltraVNC).
- RAM Scraper (Track2).
- Instant Messenger Grabber (Yahoo Messenger, Google Talk, ICQ Lite 4.x/5.x/2003, AOL Instant Messenger, Trillian, Miranda, GAIM/Pidgin, PaltalkScene, Digsby).
- Screenshots (Single, Each 30 seconds).
- Spam (Custom SMTP, html letter, unlimited email list).
- DNS Redirects (Remote host file editor).
- Persistence (Protect file, process and startup keys).
- Crypto Wallet Stealer (MultiBit, Armory, Electrum, digital, Electrum-LTC, MultiDoge, BitcoinDark, Unobtanium, Dash, Bitcoin, Litecoin, Namecoin, PPCoin, Feathercoin, NovaCoin, Primecoin, Terracoin, Devcoin, Anoncoin, Paycoin, Worldcoin, Quarkcoin, Infinitecoin,

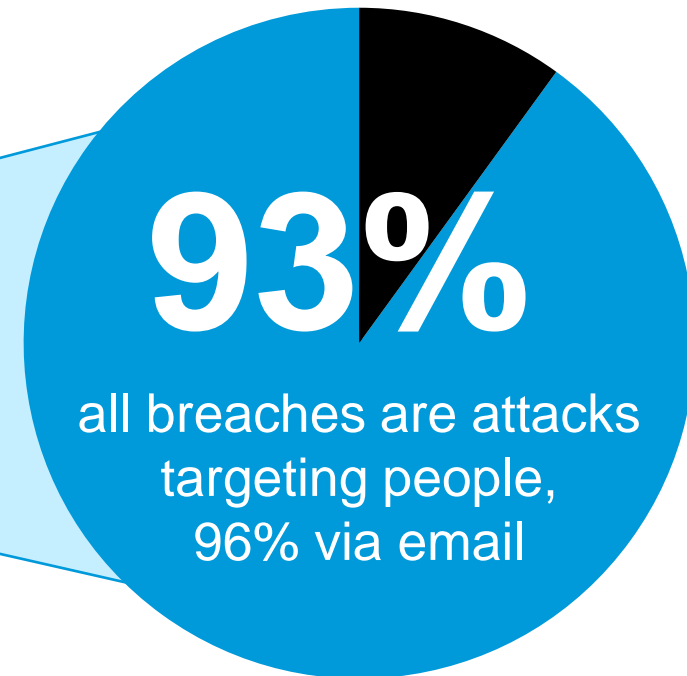
Defenders don't focus on people, Attackers do

IT Security Spending



Source: Gartner (2017 forecast)

Attack Vectors



Source: 2018 Verizon DBIR

Seehotel Jaegerwirt

- Beautiful 4 STAR hotel
- Can pay C\$634 per night
- Locked out key function and removed the capability of the hotel to open doors to rooms and make new keys
- Paid Bitcoin 2,367 C\$
- It happened 4 times.....
- Went back to manual keys ☹️

Something to Consider

Question which would be worse for an org? Ransomware or a standard data breach?

Ransomware is dead they said.....????

- 22 attacks 1st half of yr and now more than one a week
- In what is a first for Louisiana, its governor has declared a **state of emergency** after three school systems in the state were hit with cyberattacks.
- Syracuse ransomware operators **increase their demands** as victims miss payment deadlines-July 2019
- Lake City, Florida fires its IT director after **paying hackers** \$460K in ransom-June 2019
- Key Biscayne, and Riviera Beach-**600k paid out**

Ransomware is fundamentally a denial of service attack, and when services are denied to the public, it becomes a significant issue for government.

The complexity we face----Multi-staged attacks

1. Ransomware infection launched by USER opening a malicious attachment from an email
2. Attachment contained Upatre downloader
3. Downloader infected the user with GameOver Zeus
 - GameOver Zeus a stealer trojan banking/other data
4. Then Upatre would download Ryuk
5. Ryuk encrypted files and demanded a ransom

Most common point of failure is the USER

Cred Phishing as the Trigger

- Increase in phishing of enterprise cloud services
 - *dropbox, box, onedrive, salesforce...*
 - O365 phishing is a major issue
- PDFs containing links
- Not limited to email
 - *SMS, Social, etc.*
- Often the first stage of a larger attack
 - *After infiltration, remain persistent*
 - *Recon for Impostor phishing*




The image shows a screenshot of a Microsoft Outlook Web App (OWA) login page. The page has a yellow header bar with the Microsoft logo and the text "Outlook Web App (OWA)". Below the header, there is a "Security" section with a link to "show explanation". The security options are: "This is a public or shared computer" (selected with a blue radio button), "This is a private computer" (unselected with a white radio button), and "Use the light version of Outlook Web App" (unselected with a white checkbox). Below the security options, there are two input fields: "User name:" and "Password:". To the right of the "Password:" field is a "Sign in" button. At the bottom of the page, it says "Connected to Microsoft Exchange" and "© 2010 Microsoft Corporation. All rights reserved." The entire page is framed by a yellow border.

Grandcrab calling it quits in Q2?

Gandcrab

(\ /) _ (\$ _ \$) _ (\ /)

●●●●●●



Seller

424 posts

Joined

12/18/17 (ID: 84324)

Activity

virology

Posted 1 hour ago

All the good things come to an end.

For the year of working with us, people have earned more than **\$ 2 billion**, we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged **\$ 2,500,000** . We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet. We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement . We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:

1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

Ransomware crew has been in business for a couple of minutes, earned an impressive \$ 600,000. © Kaspersky

GandCrab is the most prominent ransomware of 2018. By the numbers this ransomware is huge © Check Point

The third most prevalent ransomware family. © Microsoft

GandCrab has already been made of 50K cases worldwide, so far this year © Europol

Join us -> showtopic = 136307

Cyber Fear Ransomware

You have to send money by the end of the workday, if the workday is over and people start leaving the building explosive will detonate.

will not detonate, but don't try to fool me -I guarantee you that I will withdraw my man solely after 3 confirmations in blockchain network.

behavior, panic or... the device.
I would like to suggest you a transaction. You send me 20'000 usd in Bitcoin and the device will not detonate, but don't try to fool me -I guarantee you that I will withdraw my man

Reply to All

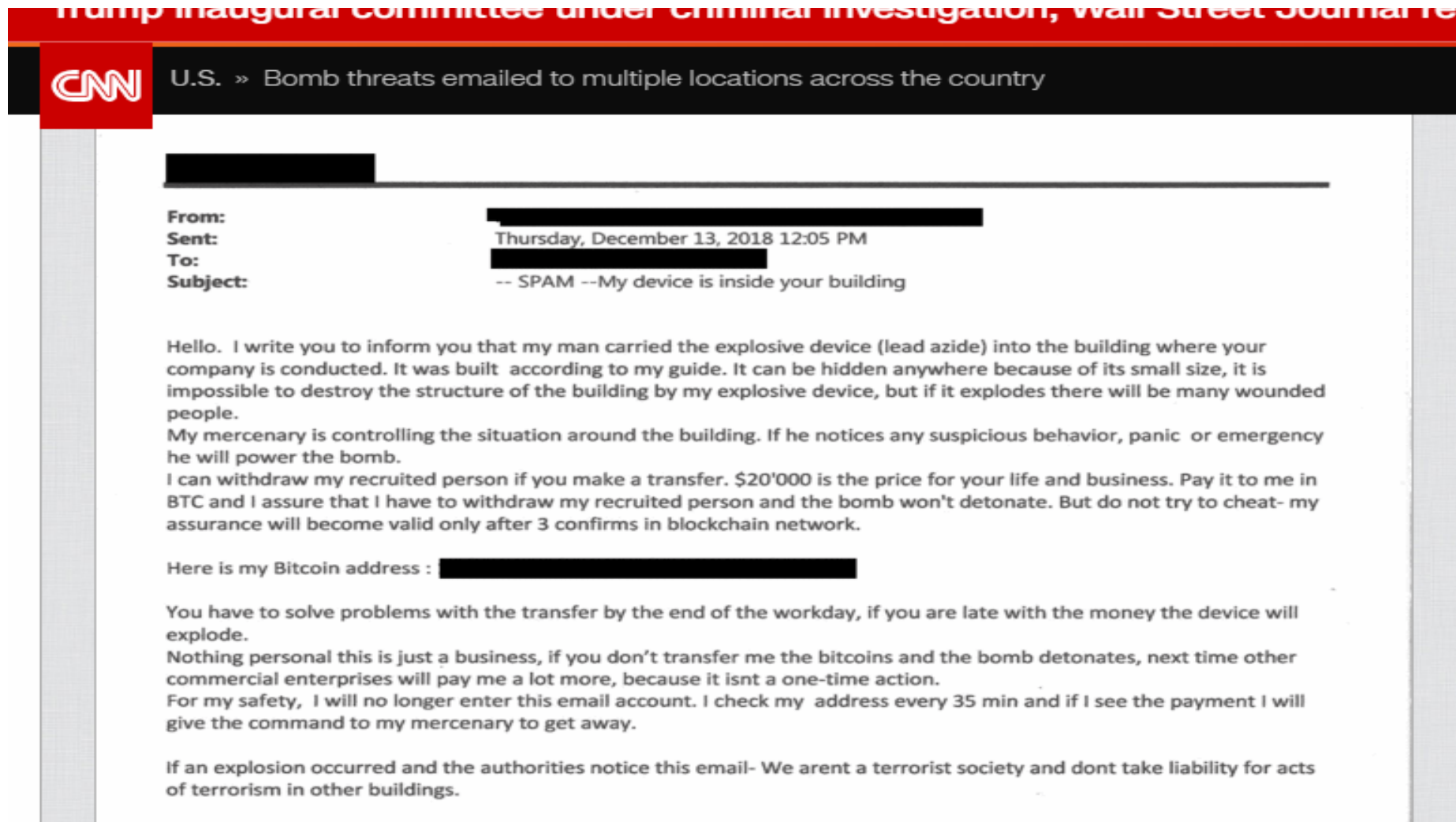
Sign in

For my safety, I wont enter this email account. I monitor my Bitcoin wallet every twenty five min and if I see the money I will give the command to my man to leave your area.

Reply to All

Sign in

This was just a year ago this occurred



Why is Ransomware returning?

- The Bitcoin Money Trail
- More distribution channels
 - Botnet network
 - Polymorphic malware
 - Malicious URL's
- Better Targets
- Cryptocurrency growth and lack of controls
- No repercussions

Baltimore

- Baltimore's "lack of investment in cybersecurity when it had already fallen victim to a similar attack" was not good for the city's credit, wrote Moody's analyst Nisha Rajan.
- *After spending more than \$10 million (hearing up to 18 million) to restore its computer networks, the city had planned paying \$835,000 to cover itself in case of future attacks*

Impact Response

- Mayors won't pay.....lets see how that goes
- IF they don't pay, they get fired. IF they pay, they get fired.
- Must have FULL backup capabilities
 - This is much easier at a local level based on the smaller size

If they don't pay, guess who is next...States and Utilities

#1 reason ransomware is distributed is email and #1 reason for infection is social engineering

To Pay or not to Pay-That is the Question....

- Paying a ransom does not guarantee an organization will regain access to their data
- Some victims who paid the demand were targeted again by cyber actors
 - (they tell their friends)
- After paying the originally demanded ransom, some victims were asked to pay more
- Having Insurance pick up the tab may cause more harm than good
- Paying could inadvertently encourage the bad behavior

Recommendations

Before the Storm

How to Prepare

- Backup and secure those backups
- Update and Patch
- Implement an awareness and training program
- Teach users how they need to respond if they get infected
- Enable strong Email Security to prevent phishing emails
- Authenticate inbound email
- Privilege account management
- Disable RDP if at all possible
- Create proper segmentation
 - Question are we connecting and automating for speed for the sake of speed or is there a real “critical value”

During the Storm

How to react

- Call law enforcement
- Disconnect from network- create break point to segment sites
- Disconnect Backup from the network too
- Change all online account passwords and network passwords
- Triage depth of infiltration
- Orchestrate Response
- Restore
 - Don't assume free tools for encryption will work (they typically don't)

After the Storm Clears

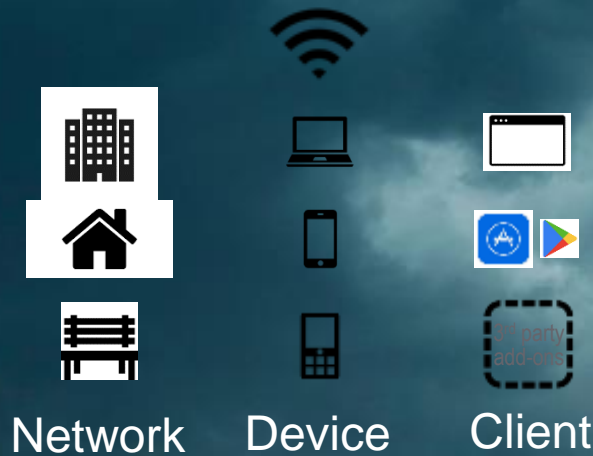
Shoring up for the next Attack

- Clean up
- Post-mortem review
- Assess User Awareness and response
- Educate on what to look for and what to do if happens
- Invest in Modern Defenses
- Focus on specifics of what the actor did, ransomware may just be a side effect

The Move to the Cloud - It's Here.....



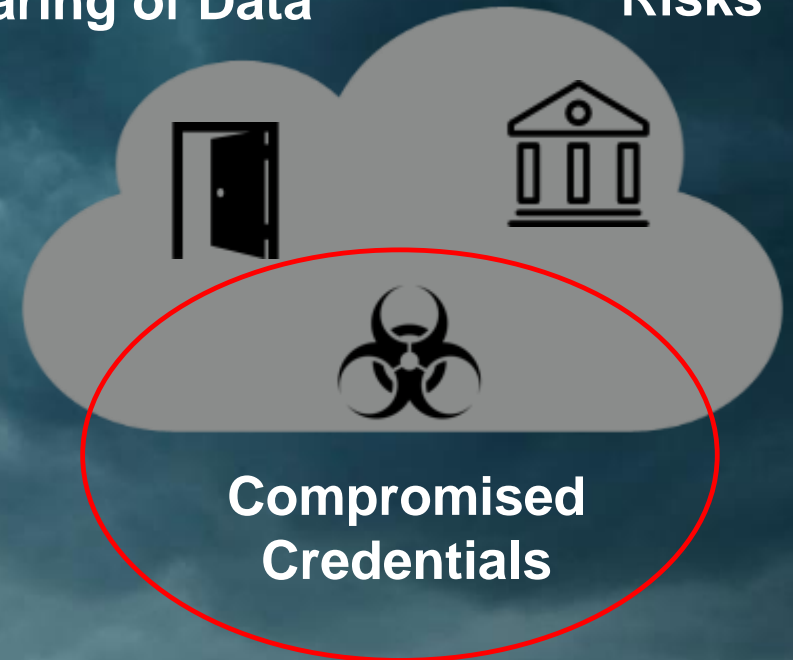
Email | Collaborate | Share Files
Download & Upload Files | Use external facing portals



ANYTIME, ANY WHERE, ANY DEVICE ACCESS

Accidental
Sharing of Data

Compliance
Risks



NEW RISKS

Layers of the Cloud

- For Revenue and Customer Communication
- Information sharing
- For Data Storage
- For Leveraging 3rd Parties to do more
- Public access cloud

Reward of Cloud

- **Reduction in cost**

- Physical costs
- Reduction in Operational and Management upkeep
- Refocus employees on more useful tasks that relate to the “actual business”
- Allow required IT components to be patched and protected in a more timely fashion
- Leveraging greater computing power resources
- Leveraging tools that allow businesses to do more
- Use third party resources as needed

- **Leveraging Other resources**

- Expertise
- Or speed to market

Risk of Cloud

- Data managed by 3rd party
- All customers in one place
 - Target for evil doers is greater
- Trust of vendors is needed
- Ramifications of Breach
- Who has access to data?

Biggest trend: Rising Wave of O365 Attacks

- Significant increase in organized attacks on O365 accounts
- Allows for INTERNAL Social manipulation
- Increasing as the Cloud move becomes larger
- Variety of techniques
 - *Brute-force appears to be the most common initial vector*
 - *Use botnets to scale across many O365 tenants*
 - *Password reuse from mega-breaches*
 - *Phishing*
- Managed Cloud - centralized data for attacker
- Rapidly developing different techniques



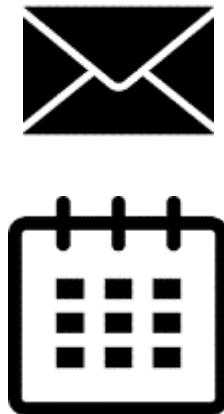
Real World Impact of Compromised Accounts

CEO's O365 Account
Compromised

Attackers
Access
Email,
Calendar

Wait for
Supplier
Meeting

Email CFO
Requesting
Wire



From: Real CEO

To: Real CFO

Stuck in this meeting. Can you send a wire to acct 5551212? It's the last thing we need to close the deal.

Bypass MFA and breach cloud accounts

- Study looked at over 100,000 logins
- 72% of tenants were targeted at least once by threat actors
- 40% of tenants had at least one compromised account in their environment
- 15 out of every 10,000 active user-accounts were successfully breached by attackers
- Attacker method was INTERNAL Phishing
- Changed forward rules or delegations to maintain persistence
- Leveraged IMAP to bypass MFA

Cloud Risks : Accidental Sharing of Sensitive Info

PFPT Findings

Files Shared Publicly

23,000

Files Shared w/ Entire Organization

300,000

Files Shared w/ Personal Accounts

8,000

by

2.5%

of users

Gaming and Hospitality – Office 365 Customer



VP of Finance
shared One Drive
directory publicly



HR shared
termination letters
with entire
organization



Sr Engineer shared
passwords w/
personal account

Proofpoint Cloud App Security Broker



Identified sensitive
data, owner and
sharing settings



Detected folders/files
shared publicly or with
entire organization



Notified user/admin
& suggested
“reduce
permissions”

Partner Network Exposure

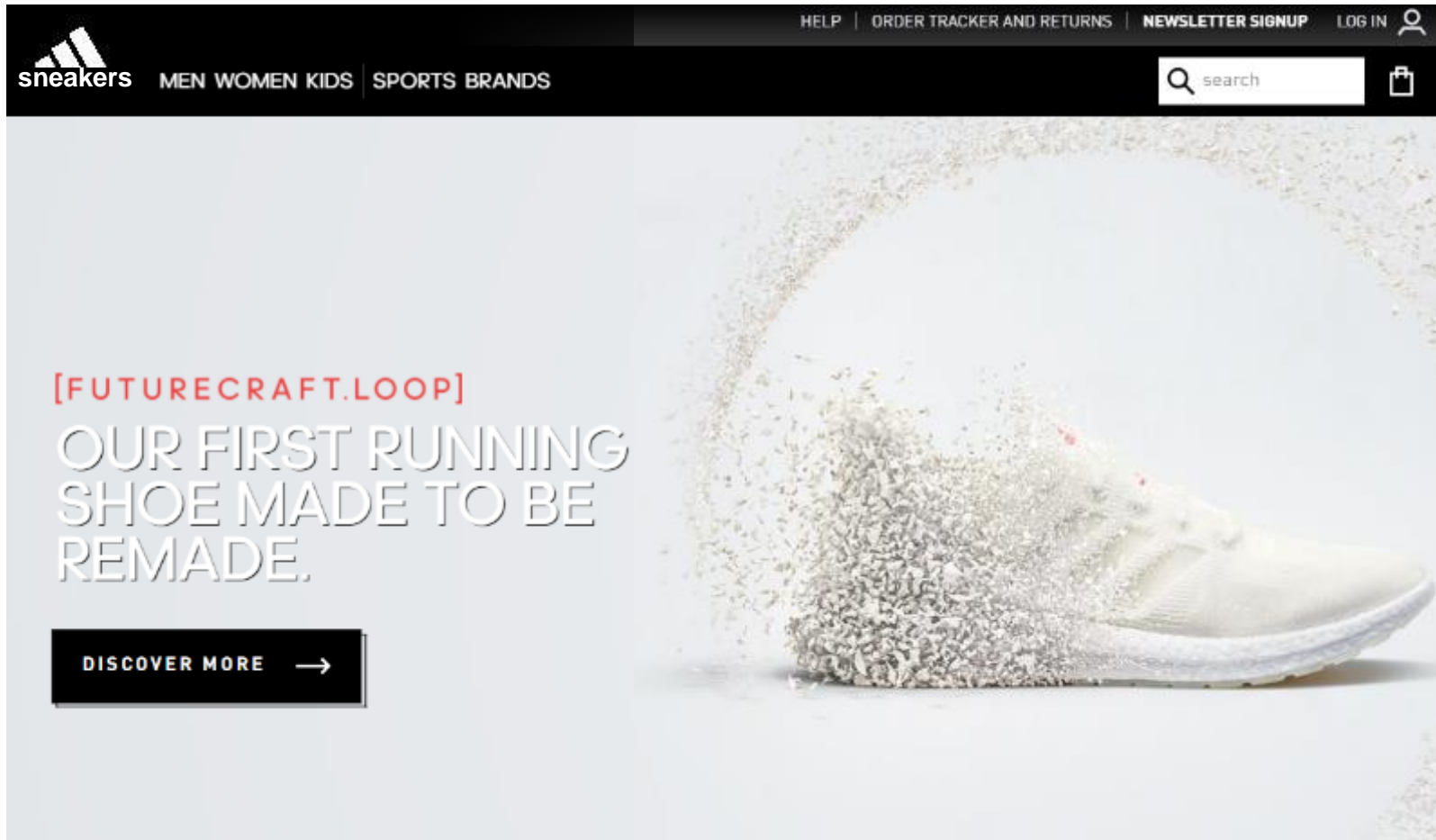
- This is a **HUGE** risk
- Fast developing organizations leveraging 3rd party partners to do more with less resources
- Partners are connected to us (VPN), Directly, Authentication
- Segmented out
- For how long are they connected? what is the specific need?
- Why doesn't it have the same level of security as the internet?

What to look for in a provider

- Physical Security
- Redundancy
- Recovery Plan
- Access control
- Data Storage
- 3rd party provider partner augmentation
- How much can you control VS the vendor
- Can you see the controls and security steps that are taken
- Listen closely to the way the vendor talks about security vs their product
- How do they hire?
- Maintenance plan and outages
- Leverage social media crowdsourcing for details on outages and recovery
- Be concerned if you ask for security details and they DON'T push back some

Leveraging Cloud with Customers

Protecting Brands from Domain Fraud



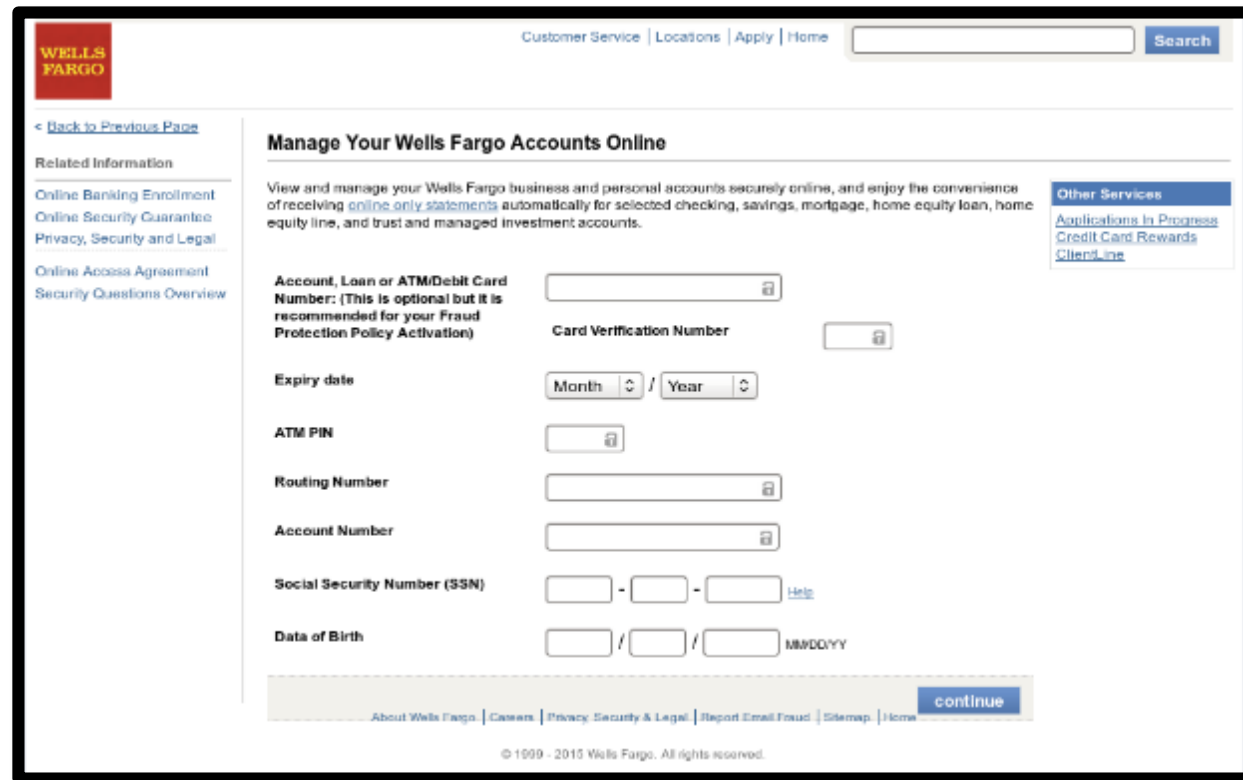
Domain Monitoring – For every well-known brand-owned domain on the internet, there are hundreds or thousands of suspicious lookalike domains potentially defrauding their customers

- No barrier to entry for domain registrations
- Variety of fraudulent techniques to imitate a brand

Protecting Brands from Social Phishing scams

@_CocoaDream: @Ask_WellsFargo what number do I call if I want to speak to someone about my account?

@WF_Helpline: @_CocoaDream Sign in at <>. You can set up a new one and move to the next page.





Isolation

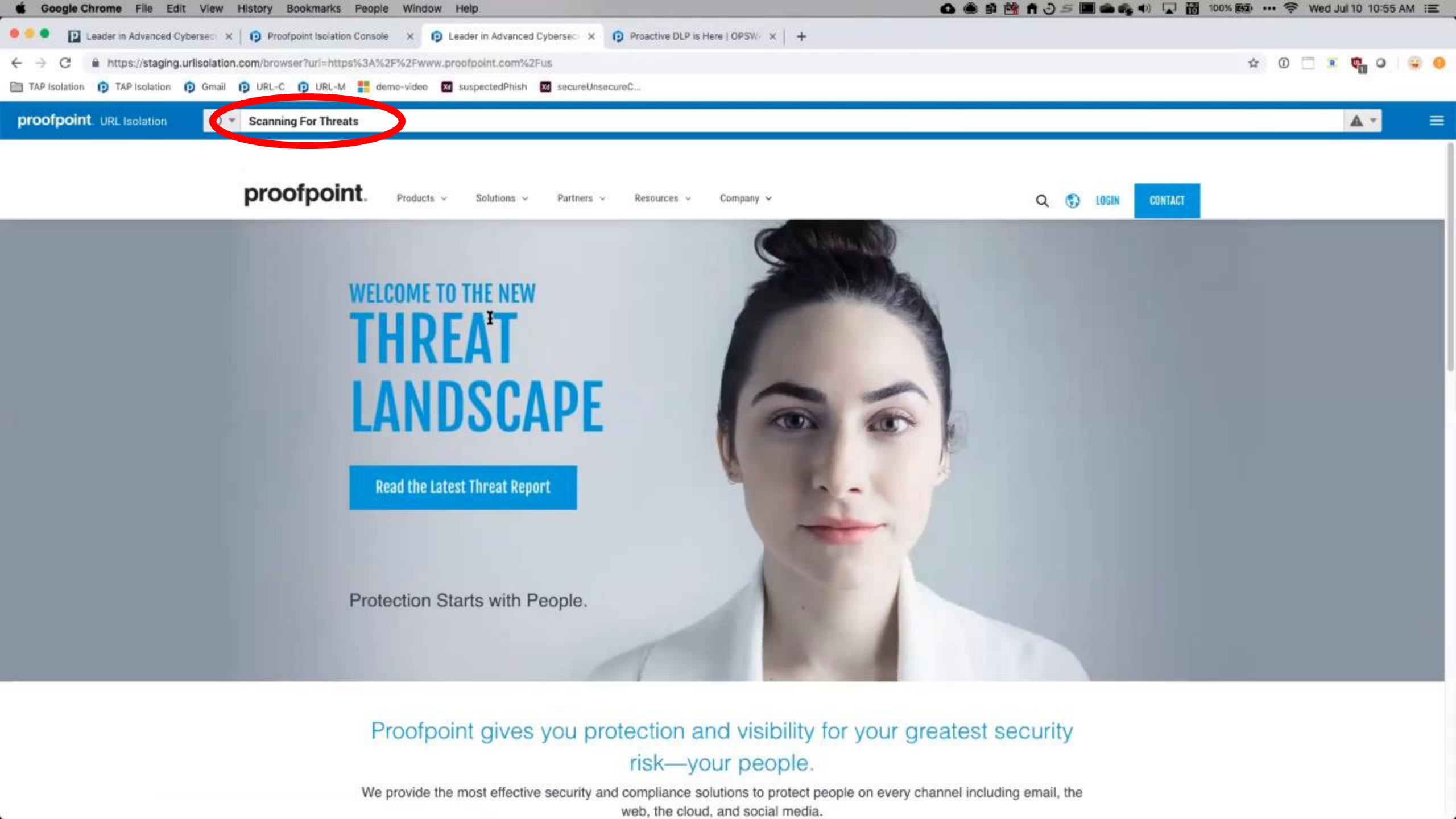
Email | Browser

- ★ Starred
- 🕒 Snoozed
- 📌 Important
- ▶ Sent
- 📧 Drafts
- 📁 new utilities
- 📁 Work
- ⌵ More

1-100 of 8,733 < >

 Promotions

<input type="checkbox"/>	☆	Washington Redskins	Pink is powerful! Kickoff to Breast Cancer Awareness Month - What is your 5-year & lifetime risk of breast cancer? View in Browser Washington Redskins ...	12:33 PM
<input type="checkbox"/>	☆	GE Appliances	Choose Your Side - Experience the Force of Innovation View this email online GE Appliances Force of Innovation Logo CHOOSE YOUR SIDE GE Appliances ...	12:21 PM
<input type="checkbox"/>	☆	The AAdvantage Dini.	Top-reviewed AAdvantage Dining restaurants - Dine out and earn AAdvantage miles. View on the web American Airlines AAdvantage Dining Hi Christophe...	11:10 AM
<input type="checkbox"/>	☆	Marriott	Free breakfast for all - Web view FAIRFIELD INN & SUITES® Marriott® FIND A HOTEL EXPLORE & PLAN MARRIOTT BONVOY Free hot breakfast daily with ...	10:59 AM
<input type="checkbox"/>	☆	BookIt.com Specials	Congratulations, Christopher! You are getting BookIt's BEST deals - Best of BookIt: Huge Savings on Top All-Inclusives + Extra \$200 Off with Coupon Cod...	8:54 AM
<input type="checkbox"/>	☆	Weltman Home Servic.	Reminder: 5 Signs That You Need To Replace Your Furnace 🔧 - Top Telltale Signs From Our HVAC Techs Call 888-457-4821 or click here to schedule ser...	8:34 AM
<input type="checkbox"/>	☆	The Home Depot	Did GE Profile Top Control Tall Tub... meet your expectations? - How many stars would you give your recent online purchase? View as web page RATE & R...	8:18 AM
<input type="checkbox"/>	☆	FTD Flowers	Surprise Them With Birthday Blooms - 20% Off - Birthdays should always be thoughtful	6:40 AM
<input type="checkbox"/>	☆	Fios	See what your DVR can do with Fios TV One - The TV you love just got better. fios✓ My Verizon Support Fios TV DVR Watch and record and record and rec...	Oct 7
<input type="checkbox"/>	☆	Expedia Fare Sale	➔ Paging passenger Chris Richmomd: You're getting the flight deal of a lifetime - You've Scored Amazing Fares Expedia.com You're on Our List for Ticke...	Oct 7
<input type="checkbox"/>	☆	Beau Rivage	Christopher, Book your Vacation Getaway to Beau Rivage this December! - Vegas Isn't Your Only Great Destination Beau Rivage Beau Rivage MGM Resort...	Oct 7
<input type="checkbox"/>	☆	HokieSports Weekly	Weekend Victories from the Hokies - This week with the Hokies! View in browser Vol. 10, No. 7 WHAT'S INSIDE: The Virginia Tech football team ended a t...	Oct 7
<input type="checkbox"/>	☆	Hotels.com	Save up to 50% - Book now and save >>	Oct 7
<input type="checkbox"/>	☆	ShopRunner	👋 Oh, hi. You have (1) friendly message: Weekly Deals - Get free 2-day shipping and returns on deals from Bloomingdale's, Tommy Hilfiger, kate spade n...	Oct 7
<input type="checkbox"/>	☆	Marriott Bonvoy	Get 30% Off Points — Up to 100,000 Points - You've got 11 more days to get points for less. My Account MARRIOTT BONVOY™ Find & Reserve redeem so...	Oct 7
<input type="checkbox"/>	☆	MileagePlus Program	Train like the real pilots do - Pilot our flight simulators in Denver. To ensure delivery to your inbox, please add MileagePlus@news.united.com to your addr...	Oct 7
<input type="checkbox"/>	☆	Charles Tyrwhitt	3 FOR \$99.95 Your favorite non-iron shirts! - Our best deal just for you View email in browser Charles Tyrwhitt - Jermyn Street, London Shirts Suits Ties ...	Oct 7
<input type="checkbox"/>	☆	Houzz	Top 71 Photos Your Neighbors Love - See what photos people near New Providence can't get enough of. People Near New Providence Are Loving These P...	Oct 7
<input type="checkbox"/>	☆	Whole Foods Market	Meet Your Local Makers—and Taste Their Food - You're Not Gonna Want to Miss This > WHOLE FOODS MARKET We Love Local. And Event...	Oct 7
<input type="checkbox"/>	☆	Riu Class	Your 15% discount is about to expire. Use it! - Loyalty Sales until 8 October If you cannot see the following email, click here Chris Richmond · Riu Class no...	Oct 7
<input type="checkbox"/>	☆	Virginia Tech Athle.	Update Regarding the Hokie Club - Letter from Whit Babcock View in browser Dear Members of the Hokie Club, Similar to how our Head Coaches of all of ...	Oct 7



Final Thoughts

- When designing, assume you will get breached, how do you minimize impact
- Watch how vendors share information and interact
 - Vendors who do cloud need to have it as part of their culture
- Don't do it just because everyone else does
- Try not to tie Apps to Cloud data
 - App organizations typically do not have strong controls
- Your users are the entry point to cloud failure so you must train them on how to use the cloud correctly
- Ensure vendors have strong monitoring and are not waiting for you to tell them there are problems