

Red Team in 2018



HITB GSEC



What is Red Team?

Military

A red team or the red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view.

3 Common Definitions

1 Open Scope

“Anything goes”, break in, social engineering, physical offices

2 Train the Blue Team

Detection and Response, assess resiliency, sparring partner

3 Objectives

Attacker / Criminal mindset, Motivations, Goals: money, espionage

The Objective is the Mission

Strategic or Tactical

Executive Management

- Overall Resiliency
- Long-term Planning and Cyber Security Strategy
- Defence Capabilities

Blue Team / Defenders

- Training and practice
- Plug holes, discover gaps

Probably not about...

XSS

Domain Admin

SQL Injection

Pass the Hash

Mimikatz

Getting ALL the
Data

Disclaimer

Law is governing our expertise is changing rapidly across the world.
Every country is creating new Cyber Security specific laws.

All techniques described should only be utilised in accordance with
law in both the source and target country.

I'm not a lawyer, make your own decisions

Vincent Yiu

SYON Security

- Service offerings driven by adversary mindset

Blog: www.vincentyi.co.uk

- Red Team Tips

CREST Certified, OSCP, OSCE

JD.com Conference, HITB GSEC, SteelCon, Bsid es Manchester, SnoopCon



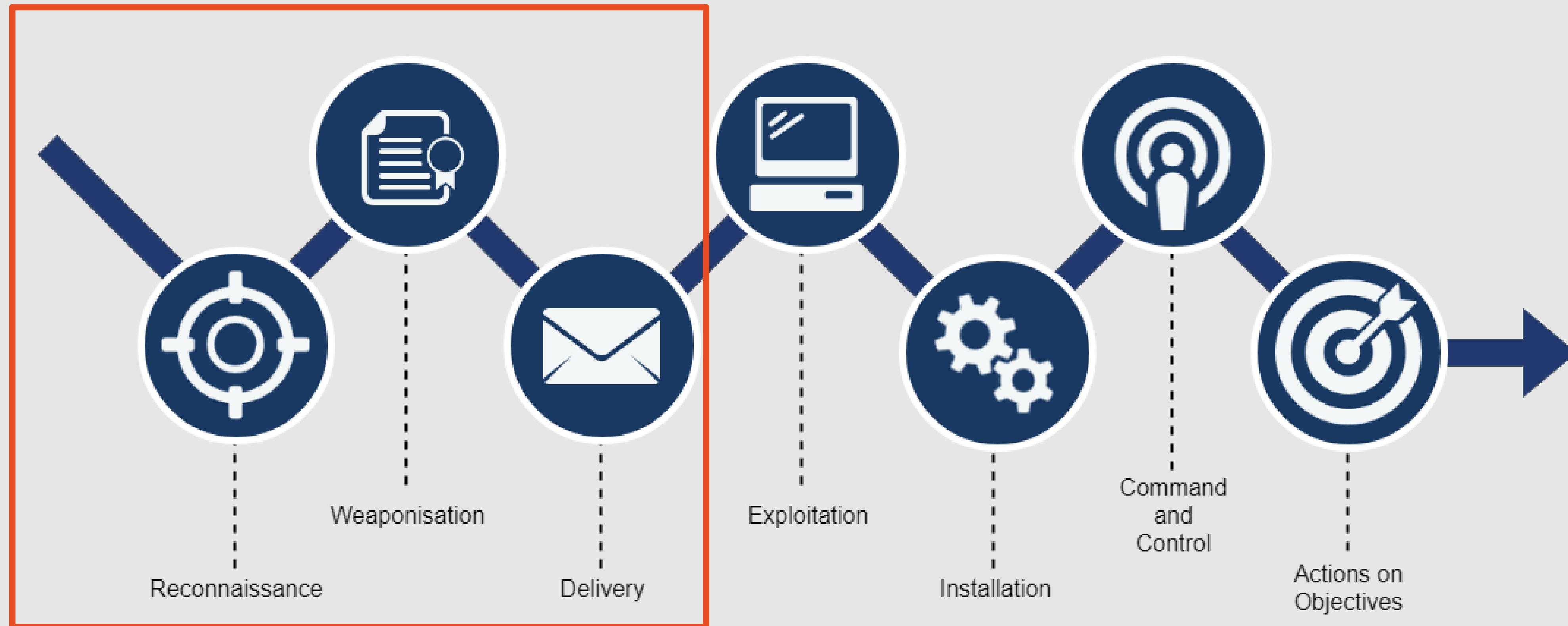
Wechat



Agenda

- Domain enumeration
- E-mail enumeration and validation
- GitHub
- Domain Fronting basics and updates
- Understanding e-mail security
- Office365

Cyber Kill Chain



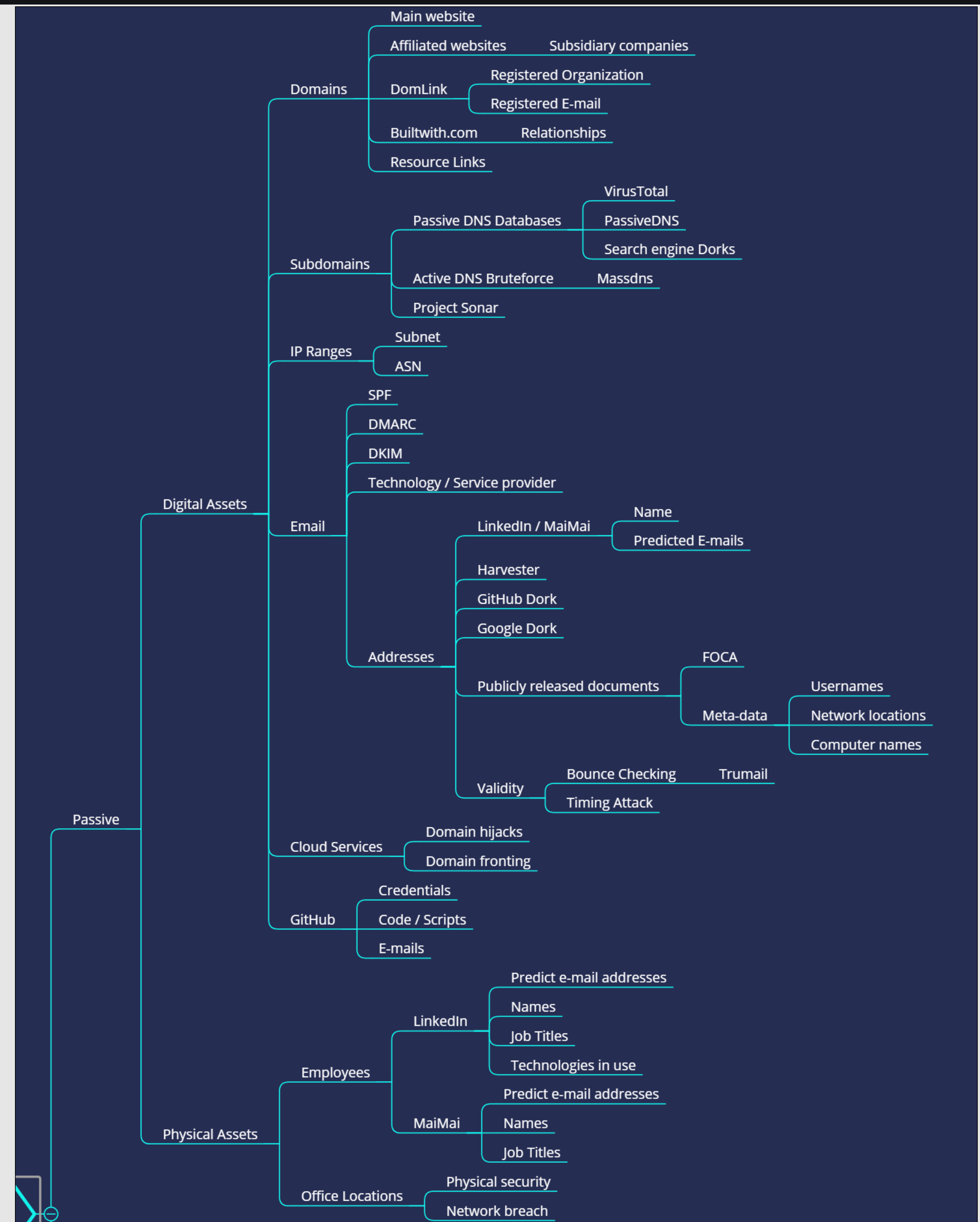
Reconnaissance

Passive Recon

- Domain enumeration
- E-mail enumeration
- E-mail attack surface discovery
- In-direct information gathering

Active Recon

- Active probing
- Has a small chance of being detected



DomLink

- Expand attack surface
- Discover additional domains

Mergers and Acquisitions

Locate Obscure Infrastructure

Used by Bug Bounty hunters (BugCrowd)

<https://github.com/vysec/domlink>

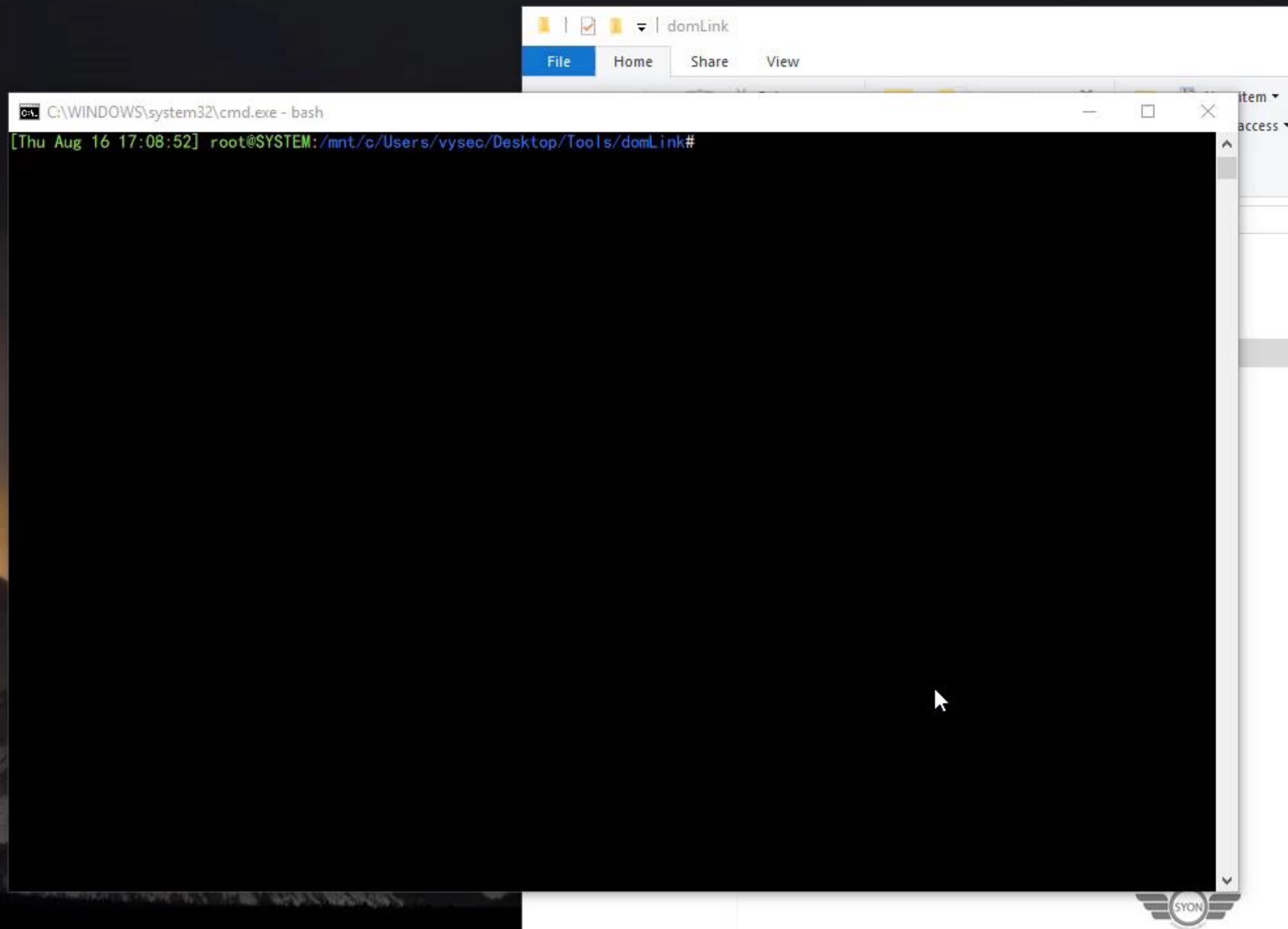
<https://vincentyi.co.uk/domlink-automating-domain-discovery/>

```
https://www.github.com/vysec/DomLink
Version: 0.1.1

Do you want to check "Uber Technologies, Inc." [Y/n]
Do you want to check "domains@uber.com" [Y/n]
Do you want to check "dev@uber.com" [Y/n]
Do you want to check "17.895.646/0001-87" [Y/n] n
Do you want to check "Uber Technologies Inc." [Y/n]
Do you want to check "Uber, Inc." [Y/n]
Do you want to check "Uber Technologies" [Y/n]
Do you want to check "UberCab, Inc." [Y/n]
Do you want to check "Uber Switzerland GmbH" [Y/n]
Do you want to check "mateo@uber.com" [Y/n]
Do you want to check "daniel.valencia@uber.com" [Y/n]
Do you want to check "arif@datomato.com" [Y/n] n
Do you want to check "herta@uber-inc.com" [Y/n]

### Company Names:
Uber Technologies Inc.
Uber Technologies, Inc.
Uber, Inc.
Uber Technologies
UberCab, Inc.
Uber Switzerland GmbH

### Domain Names:
xn--sociovia-s0a.com
uberdrivesnyc.info
```



domLink



E-mail Enumeration

Historically

- theHarvester
- Google Dorks
- Contact Pages

Social Media

- LinkedIn
- MaiMai



LinkedInt vs MailInt

LinkedInt

- Scrapes LinkedIn
- Tool released last year
- Limited to 1000 results per organization

<https://github.com/vysec/linkedint>

MailInt

- Scrapes MaiMai
- Tool released this year
- No limit on number of results
- Mainly used in China

Reverse engineered MaiMai Mobile Application

<https://github.com/vysec/maiint>

<https://vincentyi.co.uk/maiint-profiling-china-based-employees/>

```
MAILINT
MailInt V0.1 ALPHA
Author: Vincent Yiu (@vysecurity)
[*] Access Token: 1.26b22745cc007694fb1bffe108974c5b
[*] User ID: 140271776
[!] Please specify a target name (in Chinese): 唯品会
[*] Project Name: vipshop
[*] Enter e-mail domain suffix (eg. contoso.com): vipshop.com
[*] Select a prefix for e-mail generation (auto, full, firstlast, firstmlast, flast, first, last, fmlast,
auto
[*] Automatically using Hunter IO to determine best Prefix
[!] Rate limited by Hunter IO trial
[!] {first}. {last}
[+] Found first.last prefix

[*] Total number of users found: 980
[*] How many records would you like to request?: 980
[*] From what page would you like to request the 980 records? (Enter 0 for beginning): 0
[*] Requesting records 0 to 980 of 980
[*] Requesting 980 Users!
[*] Parsing Users
Found 980 users
[*] Writing CSV Report to vipshop.csv
[*] Writing HTML Report to vipshop.html
```



```
C:\WINDOWS\system32\cmd.exe - bash

C:\Users\vysec\Desktop\Tools\Mailnt_Dev>bash
[Thu Aug 16 17:25:41] root@SYSTEM:/mnt/c/Users/vysec/Desktop/Tools/Mailnt_Dev# python Mailnt.py

MAINT

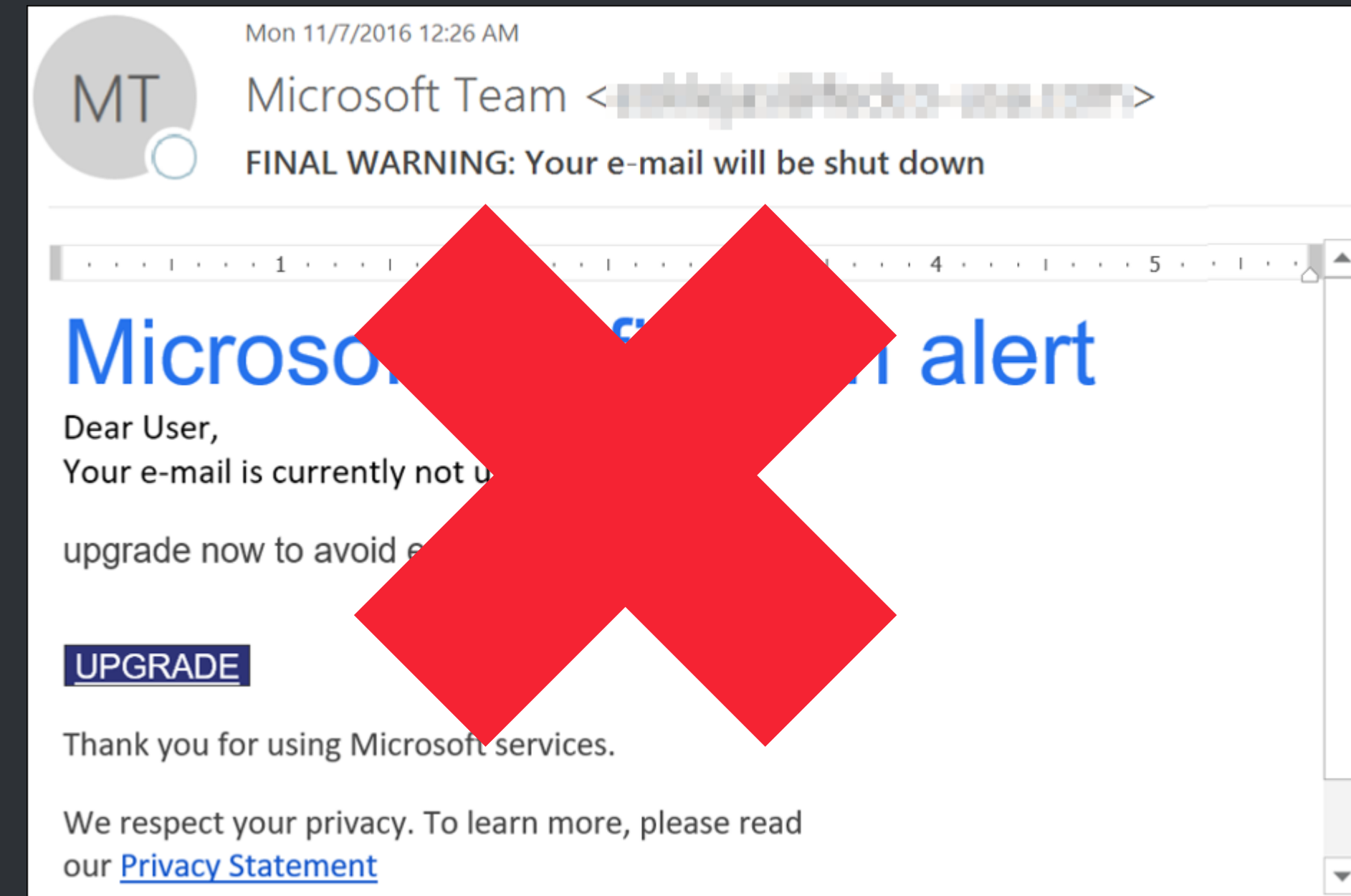
Mailnt V0.1 ALPHA
Author: Vincent Yiu (@vysecurity)
[*] Access Token: 1.26b22745cc007694fb1bffe108974c5b
[*] User ID: 140271776
[!] Please specify a target name (in Chinese):
```

Mailnt



What next? - Expectation

yingying.z
jing.zhu@
zhihao.hu
yuanyuan.
hongwei.r
juan.li@vi
jingstacy.z
zhao.liu@
guisheng.
yameng.m
lei.cai@vi
chunfan.li
gang.li@v
jianfang.li
leike.yu@
ke.lai@vip
qici.yu@v
xiaojie.he
yuchao.fu
yu.sun@v
ming.lu@v
wanbi.zha
jiahong.lin
zhenli.gao
qiuyan.lin
jianbo.su
weiyu.lin
nan.zhang
jun.fu@vi
ridong.lai
fang.huan
ming.yue
pengfei.g
chao.tan@
lin.wei@v
yazhou.lin
qianglin.a
yisen.chen
wenyuan.
xiaoling.li
xianbing.c
jingbao.gu
haohank
ruifang.ra
bingxin.ar
miaoshen
xieqian.ge
shumin.zh



What next? - Reality

yingying.z
jing.zhu@
zhihao.hu
yuanyuan.
hongwei.r
juan.li@vi
jingstacy.z
zhao.liu@
guisheng.
yameng.m
lei.cai@vi
chunfan.li
gang.li@v
jianfang.li
leike.yu@
ke.lai@vip
qici.yu@v
xiaojie.he
yuchao.fu
yu.sun@v
ming.lu@v
wanbi.zha
jiejong.lin
zhenli.gao
qiuyan.lin
jianbo.su
weiye.lin
nan.zhang
jun.fu@vi
ridong.lai
fang.huan
ming.yue
pengfei.g
chao.tan@
lin.wei@v
yazhou.lin
qianglin.a
yisen.chen
wenyuan.
xiaoling.li
xianbing.c
jingbao.gu
haohanko
ruifang.ra
bingxin.ar
miaoshen
xieqian.ge
shumin.zh



Undeliverable: Test

i Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
Outlook blocked access to the following potentially unsafe attachments: Test.

Sent Thu 16/08/2018 00:04
To Vincent Yiu
Retention Policy Junk Email (30 days) Expires 15/09/2018

Delivery has failed to these recipients or groups:

The email address you entered couldn't be found. Please check the recipient's email address and try to resend the message. If the problem continues, please contact your helpdesk.

E-mail Verification

- Bounce Checking (TruMail)
- Exchange Timing Attacks (MailSniper)
- Office365 Username Enumeration (0365enum)

Happy list of valid e-mails!

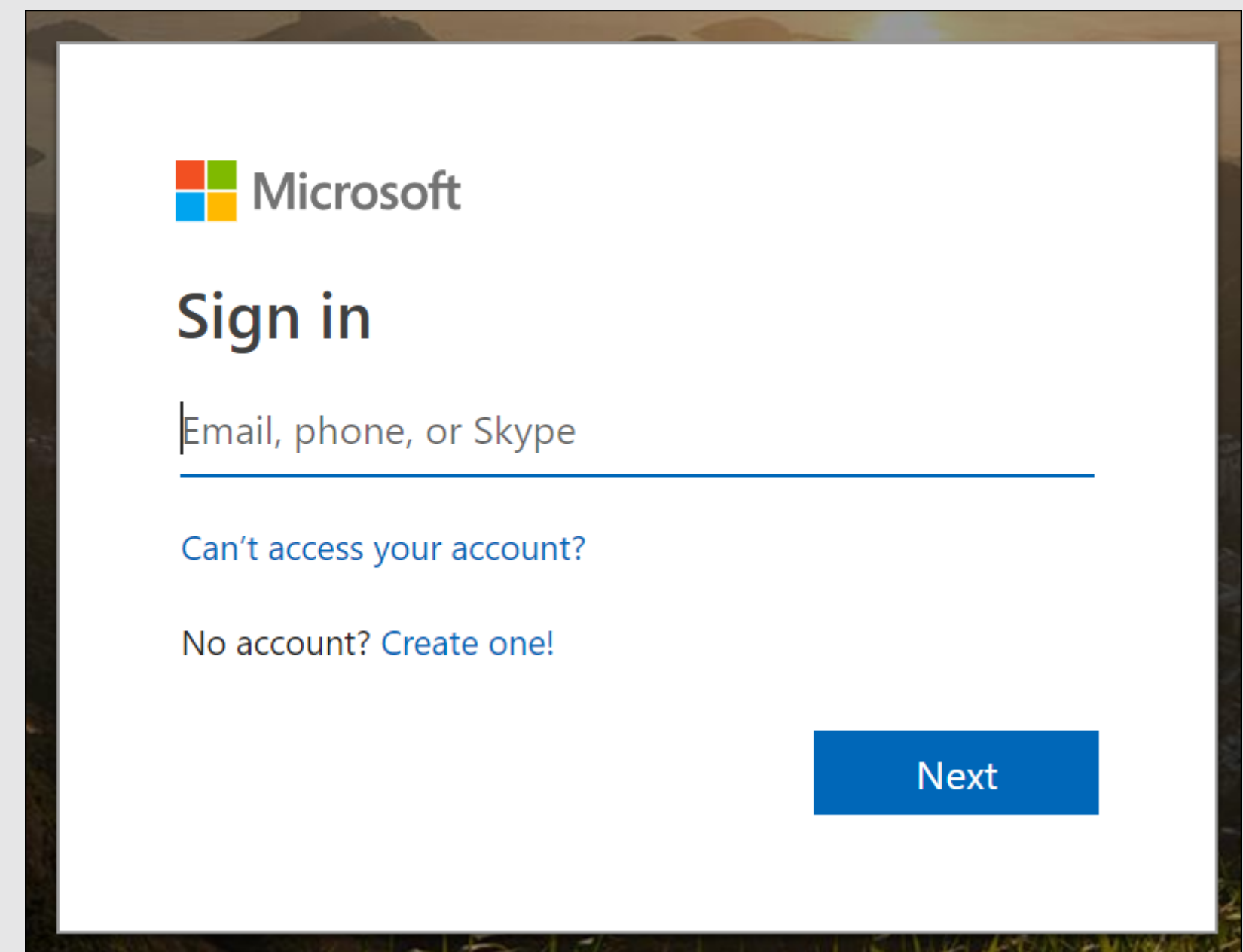
Monitoring – Active Probing

- Always use a proxy
- Multiple VPN layers if necessary

<https://github.com/sdwolfe32/trumail>

<https://github.com/dafthack/MailSniper>

<https://bitbucket.org/grimhacker/office365userenum>



Spinning up TruMail

- Free, Open Source by Sdwolfe32

Easy to Set-up

```
apt-get update
apt-get install docker
apt install docker.io
docker pull sdwolfe32/truemail
docker run -p 8080:8080 -e SOURCE_ADDR=my.email@gmail.com sdwolfe32/truemail
```

Easy to Use

<https://api.truemail.io/v2/lookups/json?email=vincent.yiu@syonsecurity.com>

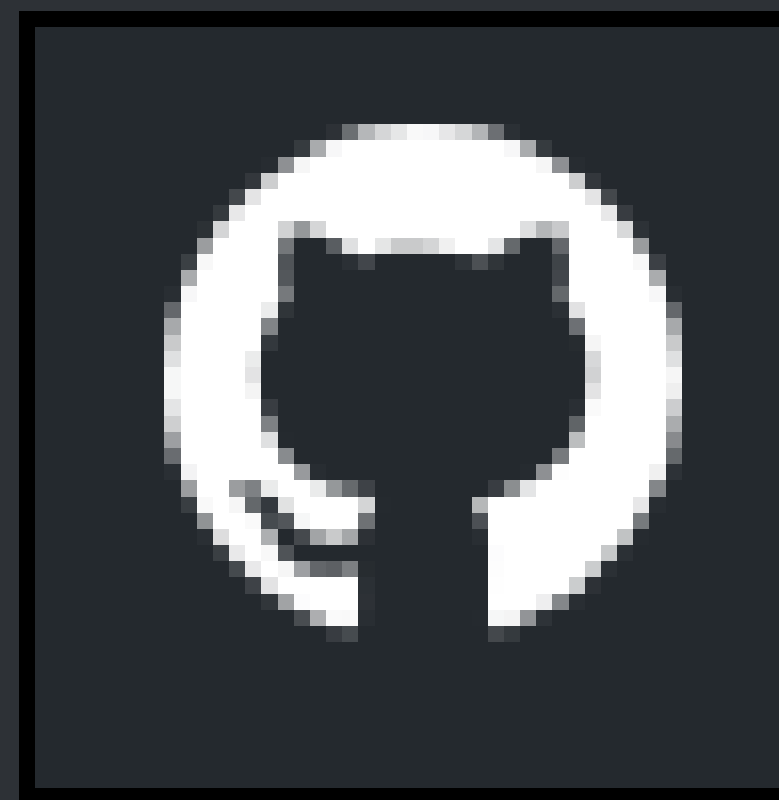
```
{"address": "vincent.yiu@syonsecurity.com", "username": "vincent.yiu", "domain": "syonsecurity.com", "md5Hash": "1e139699fc6e50712a7a970cf161c439", "suggestion": "", "validFormat": true, "deliverable": true, "fullInbox": false, "hostExists": true, "catchAll": true, "gravatar": false, "role": false, "disposable": false, "free": false}
```



<https://api.truemail.io/v2/lookups/json?email=vincent.yiu321@gmail.com>

```
{"address": "vincent.yiu321@gmail.com", "username": "vincent.yiu321", "domain": "gmail.com", "md5Hash": "3369a771a27eb48fe5c84310c92f7792", "suggestion": "", "validFormat": true, "deliverable": false, "fullInbox": false, "hostExists": true, "catchAll": false, "gravatar": false, "role": false, "disposable": false, "free": false}
```





GitHub

Massive Fails

GitHub

Useful search engine for:

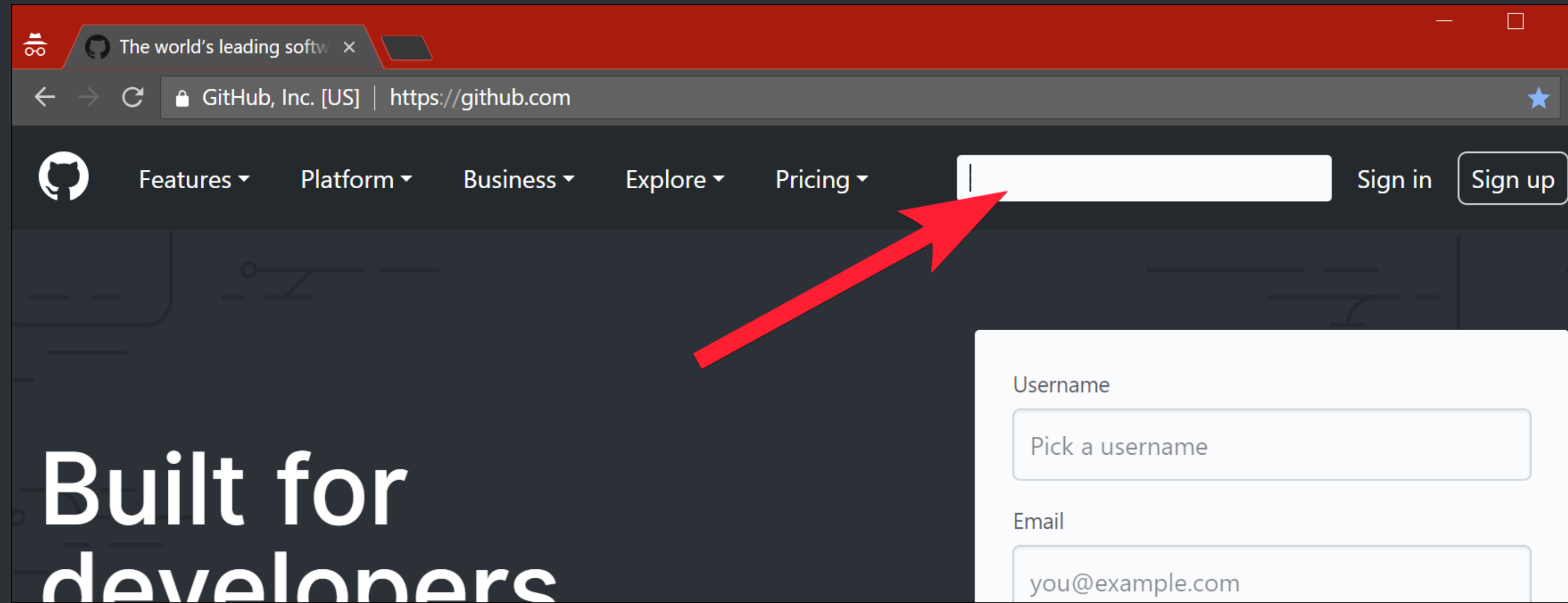
- Credentials
- Secret tokens
- Internal information
- Sysadmin notes

Operation Tips:

- Manual is best
- TruffleHog and Git secret extraction tools not great

Tooling:

- X-Patrol by Xiaomi Security Labs
<https://github.com/MiSecurity/x-patrol>
- Automated searching of GitHub
- Good for blue team and defenders
- Web Interface to audit potential leaks



“@domain.com” smtp “@domain.com” ftp

DOMEU1.corp password DOMEU1.corp intranet

DOMEU1.corp jenkins “@domain.com” password


```
1 machine gitlab.tools, [redacted]
2 login 263 [redacted]
3 password [redacted]
```

Showing the top three matches Last indexed on 17 Sep 2016

```
10 "versionTemp": "0.1.2",
11 "combohtml": "true",
12 "env": "daily",
13 "author": {
14   "name": "wangfuyang",
15   "password": "123456789",
16   "email": "shilling_wang@redacted"
17 }
18 }
```

https://github.com/CallMeYeyifei/czw/blob/e17ea34e624e1037d598ded14bfa50efad8d7f4/src/main/webapp/upload/dongxintxtfile/ZIJZ-ZJ_PS-CE08-HWNE40E.txt

```
147 local-user jiankong13805760000 password cipher %$%$vx18Lau2R#A+hpPH)L@ndyy%$%$
148 local-user jiankong13805760000 service-type terminal telnet ssh
149 local-user jiankong13805760000 level 1
150 local-user jiankong13805760000 state block fail-times 3 interval 5
151 local-user lvchang13656719537 password cipher %$%$Z2zmI[s@i1'Wyl#;>7_0ndy|)%$%$
152 local-user lvchang13656719537 service-type terminal telnet ssh
153 local-user lvchang13656719537 level 3
154 local-user lvchang13656719537 state block fail-times 3 interval 5
155 local-user pengxin15957180146 password irreversible-cipher $1a$4lc(:c*;ig$yb6-0P73g-jNb2@\'14+alk:WNCbXfc3_L#NetJDS$
156 local-user pengxin15957180146 service-type terminal telnet ssh
157 local-user pengxin15957180146 level 1
158 local-user pengxin15957180146 state block fail-times 3 interval 5
159 local-user wangfuyang15088637191 password irreversible-cipher $1a$NaqIP56Z1$y2HAIPyn3Ub_VDeO;I4@*pk-DeyZ1_3hf).0gaP$
160 local-user wangfuyang15088637191 service-type terminal telnet ssh
161 local-user wangfuyang15088637191 level 3
162 local-user wangfuyang15088637191 state block fail-times 3 interval 5
163 local-user wanglei13989817873 password cipher %$%$ps^_<C_n:"0SPGfX"+6ndyy%$%$
164 local-user wanglei13989817873 service-type terminal telnet ssh
165 local-user wanglei13989817873 level 3
166 local-user wanglei13989817873 state block fail-times 3 interval 5
167 local-user wangqian15925615178 password cipher %$%$_$4lG7nEtEbq@Pc|)[&*ndy%$%$
168 local-user wangqian15925615178 service-type terminal telnet ssh
169 local-user wangqian15925615178 level 3
170 local-user wangqian15925615178 state block fail-times 3 interval 5
171 local-user wangyfaaaa13868005225 password cipher %$%$Z"TVxSYnHT"TO[VW/^FnnDy%$%$
172 local-user wangyfaaaa13868005225 service-type terminal telnet ssh
173 local-user wangyfaaaa13868005225 level 3
```

```
1 account default
2 host smtp [redacted]
3 port 465
4 from [redacted]
5 auth on
6 tls on
7 tls_starttls off
8 tls_trust_file /etc/ssl/certs/ca-certificates.crt
9 user lcl [redacted]
10 password [redacted]
11 logfile /tmp/msmtp.log
```

```
2 spring.datasource.url=jdbc:mysql://[redacted]:[redacted]:[redacted]
3 spring.datasource.username=[redacted]
4 spring.datasource.password=[redacted]
```

```
6 spring.jpa.database-platform=org.hibernate.dialect.MySQL5InnoDBDialect
```

```
17 #spring.mvc.view.prefix=/static/
18 #spring.mvc.view.suffix=.jsp
19
20 ## MULTIPART (MultipartProperties)
21 # Enable multipart uploads
```

```
1724 ip route-static vpn-instance ChinaMobile_GPRS_ZX 10.72.252.250 255.255.255.255 10.72.252.12 description LTE-ZX
1725 ip route-static vpn-instance ChinaMobile_GPRS_ZX 10.72.252.252 255.255.255.255 10.72.252.12 description LTE-ZX
1726 ip route-static vpn-instance ChinaMobile_GPRS_ZX 10.76.0.1 255.255.255.255 10.72.252.12 description LTE-ZX
1727 ip route-static vpn-instance ChinaMobile_IUPS_Media 10.74.5.0 255.255.255.0 NULL0
1728 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.236.128 255.255.255.128 NULL0
1729 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.0 255.255.255.192 NULL0
1730 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.1 255.255.255.255 Vlanif1085 192.168.19.98 track bfd-session sgsn39_0/13/1 d
1731 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.2 255.255.255.255 Vlanif1085 192.168.19.98 track bfd-session sgsn39_0/13/1 d
1732 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.3 255.255.255.255 Vlanif1085 192.168.19.99 track bfd-session sgsn39_1/12/1 d
1733 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.4 255.255.255.255 Vlanif1085 192.168.19.99 track bfd-session sgsn39_1/12/1 d
1734 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.5 255.255.255.255 Vlanif1085 192.168.19.100 track bfd-session sgsn39_1/13/1
1735 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.6 255.255.255.255 Vlanif1085 192.168.19.100 track bfd-session sgsn39_1/13/1
1736 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.7 255.255.255.255 Vlanif1105 192.168.19.130 track bfd-session sgsn40_0/13/1
1737 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.8 255.255.255.255 Vlanif1105 192.168.19.130 track bfd-session sgsn40_0/13/1
1738 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.9 255.255.255.255 Vlanif1105 192.168.19.131 track bfd-session sgsn40_1/12/1
1739 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.10 255.255.255.255 Vlanif1105 192.168.19.131 track bfd-session sgsn40_1/12/1
1740 ip route-static vpn-instance ChinaMobile_IUPS_Media 112.58.238.11 255.255.255.255 Vlanif1105 192.168.19.132 track bfd-session sgsn40_1/13/1
```

src/main/webapp/upload/dongxintxtfile/ZJHUZ-PA-T-SW09-EH2F-S2352.txt

Showing the top two matches Last indexed 16 days ago

```
11 super password level 3 cipher F*OJ+[T'MaOQ="Q'MAF4<1!!
12
13 #
14
15 vlan batch 1 3888 4088
16
17 #
18
19 cluster enable
...
83 domain default_admin
84
85 local-user admin password simple admin
86
87 local-user admin service-type http
88
89 local-user boc04 password cipher ``7=U;$B"/GQ="Q'MAF4<1!!
```

target/dnbm-maven-0.0.1-SNAPSHOT/upload/dongxintxtfile/ZJHUZ-PA-T-SW09-EH2F-S2352.txt

Showing the top two matches Last indexed 16 days ago

```
11 super password level 3 cipher F*OJ+[T'MaOQ="Q'MAF4<1!!
12
13 #
14
15 vlan batch 1 3888 4088
16
17 #
18
19 cluster enable
...
83 domain default_admin
84
85 local-user admin password simple admin
86
87 local-user admin service-type http
```

https://github.com/CallMeYeyifei/czw/tree/e17ea34e624e1037d598ded14bfa50efad8d7f4/src/main/webapp/upload/dongxintxtfile

CallMeYeyifei / czw			Watch 0	Star 0	Fork 0
Code	Issues 0	Pull requests 0	Projects 0	Wiki	Insights
Tree: e17ea34e2 czw / src / main / webapp / upload / dongxintxtfile /					
CallMeYeyifei 未认证 21 days ago					
..					
SSL-VPN-FW.txt	承载网	21 days ago			
ZJHUZ-BA-IPNET-RT01-GSR12416.txt	承载网	21 days ago			
ZJHUZ-BA-IPNET-RT02-GSR12416.txt	承载网	21 days ago			
ZJHUZ-BA-ZL-PS-RT01-GSR12410.txt	承载网	21 days ago			
ZJHUZ-BA-ZL-PS-RT02-GSR12410.txt	承载网	21 days ago			
ZJHUZ-MC-WGDCN-SW01-FH2F-S9306.txt	承载网	21 days ago			
ZJHUZ-MC-WGDCN-SW02-EH2F-S9306.txt	承载网	21 days ago			
ZJHUZ-NGN-CE01-CISCO7609.txt	承载网	21 days ago			
ZJHUZ-NGN-CE02-CISCO7609.txt	承载网	21 days ago			
ZJHUZ-NGN-CE03-HWNE40E.txt	承载网	21 days ago			
ZJHUZ-NGN-CE04-HWNE40E.txt	承载网	21 days ago			
ZJHUZ-NGN-CE05-CISCO7609.txt	承载网	21 days ago			
ZJHUZ-NGN-CE06-CISCO7609.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW01-EH6F-S3928P.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW02-EH7F-S3328P.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW03-FHL2F-S3352P.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW04-EH5F-S3352P.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW05-EH11F-S3352P.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW06-EH5F-S3900P.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW07-EH5F-S3900P.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW09-EH2F-S2352.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW10-EH2F-S2352.txt	承载网	21 days ago			
ZJHUZ-PA-T-SW11-FH2F-S3352P.txt	承载网	21 days ago			
ZJHUZ-PA-WGDCN-SW01-FH2F-S3550.txt	承载网	21 days ago			
ZJHUZ-PA-WGDCN-SW02-FH2F-S3550.txt	承载网	21 days ago			
ZJHUZ-BA-WGDCN-SW01-FH2F-S3300P.txt	承载网	21 days ago			



Weaponization

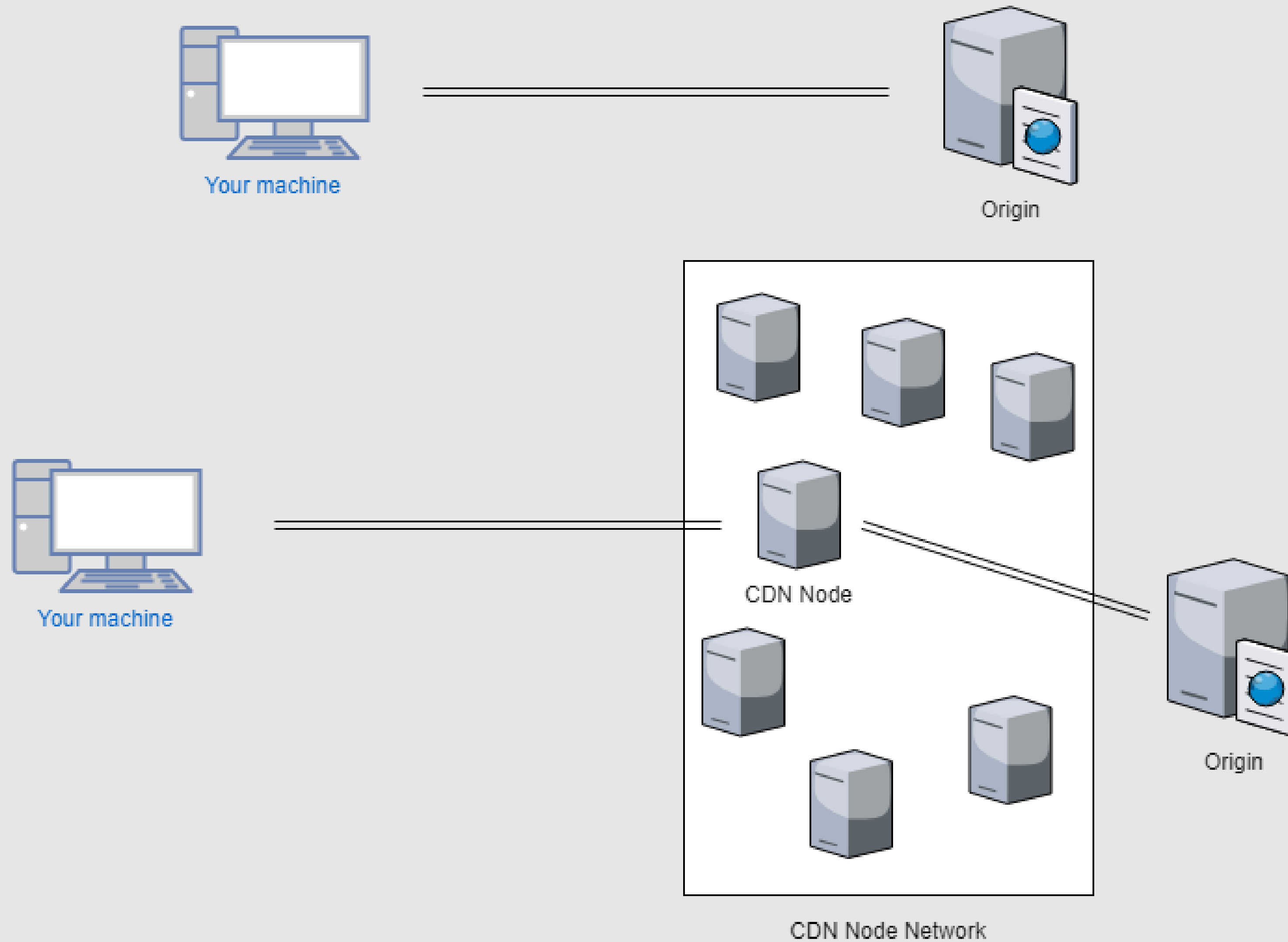


Focus on Command and Control

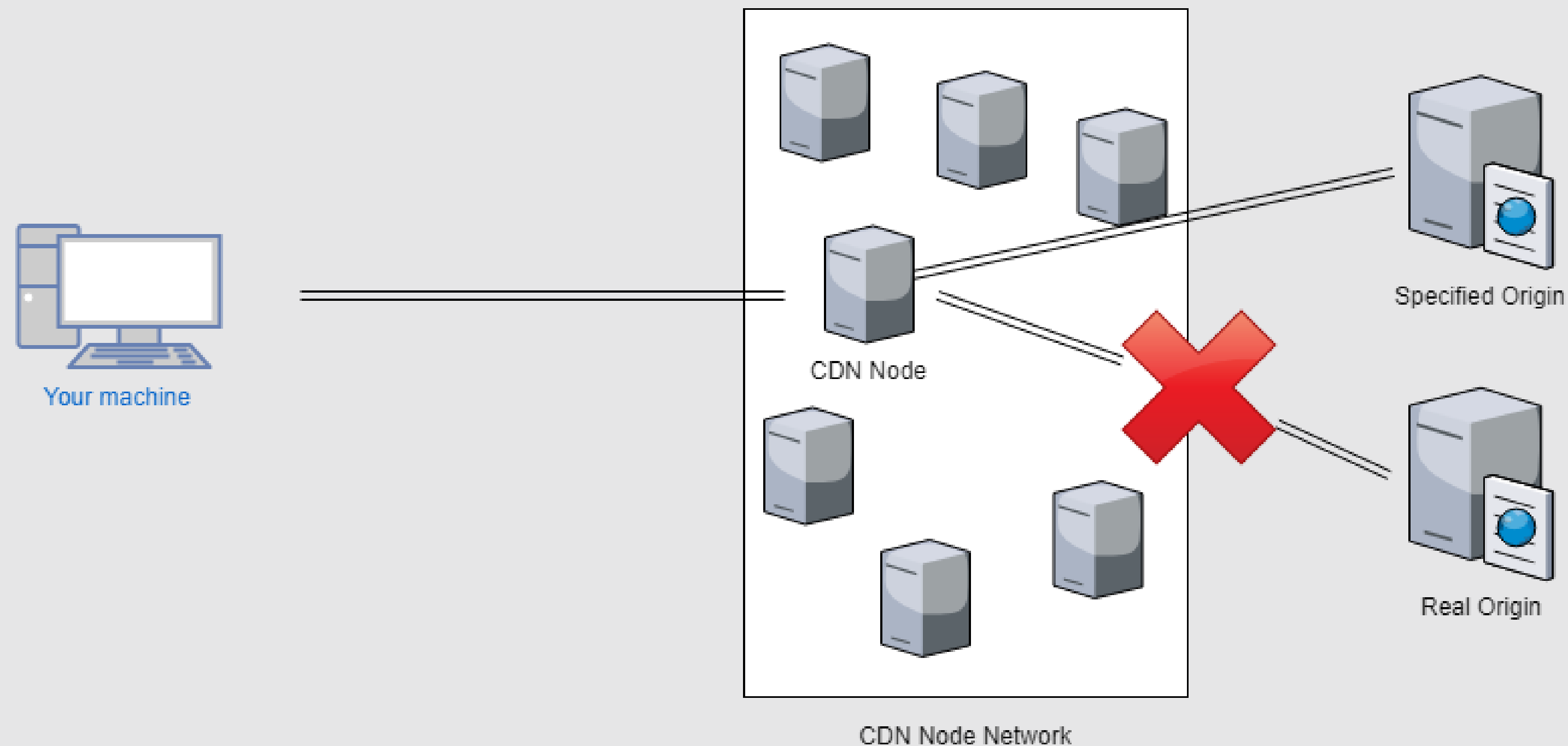
Domain Fronting

Is it dead?
I heard it's on it's way out...

CDN Basics



Domain Fronting



Normal flow of traffic

DNS Request for `www.gotomeeting.com`

GET / HTTP/1.1

Host: `www.gotomeeting.com`


Domain Fronting flow of traffic

DNS Request for `www.gotomeeting.com`

GET / HTTP/1.1

Host: `nice.try.but.no`

It's dead!!!

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE FOR

THAT'S NOT A FEATURE, IT'S A BUG —

Google disables “domain fronting” capability used to evade censors

A "long-planned" change happens to coincide with a new wave of state censorship in Russia.

SEAN GALLAGHER - 4/20/2018, 1:57 AM


THE VERGE TECH SCIENCE CULTURE MORE f t r u q

GOOGLE POLICY & LAW US & WORLD

A Google update just created a big problem for anti-censorship tools ¹⁸

Domain-fronting is now a thing of the past


By Russell Brandom | @russellbrandom | Apr 18, 2018, 4:55pm EDT

SECURITY 

As Google and AWS kill domain fronting, users must find a new way to fight censorship

The messaging app Signal used a technique called domain fronting to misdirect censors in certain regions.

By James Sanders | May 2, 2018, 5:16 AM PST

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

SIGNAL DROP —

Amazon blocks domain fronting, threatens to shut down Signal’s account

Move makes evasion of Middle Eastern countries' censorship of Signal more difficult.

SEAN GALLAGHER - 5/3/2018, 2:50 AM

Quotes!

As privacy advocates fretted, Google was adamant that fronting had always been an accidental feature:

Domain fronting has never been a supported feature at Google but until recently it worked because of a quirk of our software stack. We're constantly evolving our network, and as part of a planned software update, domain fronting no longer works. We don't have any plans to offer it as a feature.

Three weeks on and Amazon has given Signal the knock-back in a brusque email the app developer has made public:

We are happy for you to use AWS Services, but you must comply with our Service Terms. We will immediately suspend your use of CloudFront if you use third party domains without their permission to masquerade as that third party.

CDN Vendors

Domain Frontable:

- Google
- Google Hosted
- Amazon CloudFront
- Azure
- Alibaba Cloud
- Baidu
- Oppo
- Many more...



Google Compute Engine



Google

Google App Engine – Front:

- `www.google.com`
- `mail.google.com`

The Old:

Host: `*..appspot.com`
– rejected over HTTPS

```
[Thu Aug 16 05:22:57] root@msft: ~# curl https://www.google.com --header "Host: webaut
.appspot.com"
<html><body><h1>502 Bad Gateway</h1><p>This HTTP request has a Host header that is no
red by the TLS certificate used. Due to an infrastructure change, this request cannot
ocessed.</p></body></html>
```



Google Compute Engine

The New:

Host: `c.storage.googleapis.com`

Host: `storage.l.googleusercontent.com`

```
root@localhost: # curl https://www.google.com/index.html --header "Host: ctmirror.storage.googleapis.com" | head -n 100
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
  0     0     0     0     0     0     0      0      0     0  --:--:-- --:--:-- --:--:--    0<!--
@license
Copyright (c) 2016 The Polymer Project Authors. All rights reserved.
This code may only be used under the BSD style license found at http://polymer.github.io/LICENSE.txt
The complete set of authors may be found at http://polymer.github.io/AUTHORS.txt
The complete set of contributors may be found at http://polymer.github.io/CONTRIBUTORS.txt
Code distributed by Google as part of the polymer project is also
subject to an additional IP rights grant found at http://polymer.github.io/PATENTS.txt
-->

<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="description" content="Google Codelabs">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <meta name="generator" content="Google Codelabs">
  <meta name="application-name" content="Google Codelabs">
  <title>Google Codelabs</title>

  <link rel="manifest" href="manifest.json">
  <link rel="shortcut icon" sizes="192x192" href="images/touch/icon_192.png">

  <!-- Add to homescreen for Safari on iOS -->
  <meta name="apple-mobile-web-app-capable" content="yes">
  <meta name="apple-mobile-web-app-status-bar-style" content="#37474F">
  <meta name="apple-mobile-web-app-title" content="Google Codelabs">
  <link rel="apple-touch-icon" href="images/touch/icon_144.png">

  <!-- Win 8 -->
  <meta name="msapplication-TileImage" content="images/touch/icon_144.png">
  <meta name="msapplication-TileColor" content="#37474F">

  <link rel="stylesheet" href="styles/main.css">
```



Google Hosted

<https://github.com/vysec/DomainFrontingLists/blob/master/Google-hosted-SSL.txt>



Google Compute Engine

Many websites using App Engine

- Including Health, and Government

```
C:\Users\vysec\Desktop\Tools\DomainFrontingLists>type Google-hosted-SSL.txt | findstr /i .gov
[!] SSL Front: coral.aims.gov.au
[!] SSL Front: crimenmexico.diegovalle.net
[!] SSL Front: eesasupport.lbl.gov
[!] SSL Front: gcr.onegovcloud.com
[!] SSL Front: ivan.ochagov.net
[!] SSL Front: weather.aims.gov.au
[!] SSL Front: www.arctic.gov
[!] SSL Front: www.diegovalle.net
[!] SSL Front: www.foi.gov.ph
[!] SSL Front: www.mandauecity.gov.ph
```

Host: *.appspot.com

```
root@localhost:~# curl https://www.curablehealth.com --header "Host: kanban-chi.appspot.com"
<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, maximum-scale=1, viewport-fit=cover" />
  <title>Error 404 (Not Found)!!!</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px sans-serif}body{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 0 30px}@media(max-width:390px){background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px 0}@media(max-width:390px){padding:5px 0}code{background:#f7f7f7;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;border-left:5px solid #4285f4}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;border-left:5px solid #4285f4}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;webkit-background-size:100% 100%}}#logo{display:inline-block;height:54px;vertical-align:middle;width:150px}}
  </style>
  <a href=/www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>404.</b> <ins>That's an error.</ins>
  <p>The requested URL <code>/</code> was not found on this server. <ins>That's all we know.</ins>
```

```
C:\Users\vysec\Desktop\Tools\DomainFrontingLists>type Google-hosted-SSL.txt | findstr /i health
[!] SSL Front: api.kickhealth.co
[!] SSL Front: balancebeautyandhealth.leadpages.net
[!] SSL Front: designerhealthcenters.leadpages.net
[!] SSL Front: dignityhealth.optimizehit.com
[!] SSL Front: es.kentucky.aetnabetterhealth.com
[!] SSL Front: es.virginia.aetnabetterhealth.com
```

What works:

Host: customdomain.com

Settings

Application settings
Custom domains
SSL certificates
Email senders

Add a custom domain
Enable managed security
Disable managed security

i All domains mapped to this application are shown below. Only owners of a domain may remove one of its mappings.

<input type="checkbox"/> Custom domain name ^	SSL security	Certificate ID	Record type	Data	Alias	
<input type="checkbox"/> *.tealab.space	none	-	CNAME	ghs.googlehosted.com	*	
<input type="checkbox"/> tealab.space	Google-managed, auto-renewing	-	A	216.239.32.21	(none)	
			A	216.239.34.21		
			A	216.239.36.21		
			A	216.239.38.21		
			AAAA	2001:4860:4802:32::15		
			AAAA	2001:4860:4802:34::15		
			AAAA	2001:4860:4802:36::15		
			AAAA	2001:4860:4802:38::15		
<input type="checkbox"/> www.tealab.space	Google-managed, auto-renewing	-	CNAME	ghs.googlehosted.com	www	



Amazon CloudFront



Against Terms of Service 
USE AT OWN RISK

- Still works, no changes
- Largest selection of domains for fronting to date
- Can have an arbitrary non-existent host header of your choice

<https://vincentyiu.co.uk/domain-fronting-who-am-i/>

<https://vincentyiu.co.uk/validated-cloudfront-ssl-domains/>

<https://github.com/vysec/DomainFrontingLists/blob/master/CloudFront-SSL.txt>

Azure



- Microsoft owned
- Growing in popularity, adoption starting to surpass Amazon Web Services
- Domain Fronting works

<https://theobsidiantower.com/>

Has Microsoft domains:

- `csr1.microsoft.com`, `do.skype.com`

Has Customer domains:

```
C:\Users\vysec\Desktop\Tools\DomainFrontingLists>type Azure.txt | findstr /i go
gov.iris.net
gov.mywebvalet.net
www2.health.gov.il
www.minhacasaminhvida.gov.br
```

<https://github.com/vysec/DomainFrontingLists/blob/master/Azure.txt>

```
# cat known-good.txt | grep microsoft | grep -v goskope
*.Applicationinsights.microsoft.com
*.manage.microsoft.com
*.media.microsoftstream.com
*.microsoft-sbs-domains.com
*.microsoft.com
*.mp.microsoft.com
*.s.windows.microsoft.com
ajax.microsoft.com
cdn.wallet.microsoft-ppe.com
cdn.wallet.microsoft.com
download.learningdownloadcenter.microsoft.com
download.visualstudio.microsoft.com
lumiahelptipscdn.microsoft.com
lumiahelptipscdnqa.microsoft.com
lumiahelptipsmscdn.microsoft.com
lumiahelptipsmscdnqa.microsoft.com
mscrl.microsoft.com
r20swj13mr.microsoft.com
software-download.coem.microsoft.com
software-download.microsoft.com
software-download.office.microsoft.com

# cat known-good.txt | grep skype | grep -v goskope
*.cdn.skype.com
*.cdn.skype.net
*.dev.skype.com
*.secure.skypeassets.com
*.secure.skypeassets.net
do.skype.com
```



Other Vendors

All support Domain Fronting
Videos on YouTube

 Alibaba Cloud



TLS Inspection

- Monitor employees and inspect for malicious traffic
- Legal and Compliance
 - HIPAA – Health category not inspected
- Implicit Trust in Health, Government, Financial websites
- Performance Issues
 - Major sites not inspected

Default Exemptions



@n00py1 published <https://pastebin.com/raw/Fa0nqg5g>

Palo Alto vs. Domain Fronting

Cross-referenced to CloudFront Domain Fronts

Mozilla
Citrix
GoToMeeting
Periscope
Line (Korean chat app)

```
← → ↻ 🔒 https://pastebin.com/raw/Fa0nqg5g

Hostname
*.*.logmein.com
*.agent.datadog.com
*.agni.lindenlab.com
*.airddroid.com
*.ams.citrixonline.com
*.atl.citrixonline.com
*.bitdefender.com
*.bitdefender.net
*.ciscospark.com
*.citrixonlinecdn.com
*.cloudmosa.com
*.courier.sandbox.push.apple.com
*.dochub.com
*.dropcam.com
*.ess.apple.com
*.fra.citrixonline.com
*.gc.apple.com
*.gotomeeting.com
*.iad.citrixonline.com
*.icloud.com
*.informaticacloud.com
*.informaticaondemand.com
*.itunes.apple.com
*.itwin.com
*.kakao.com
*.las.citrixonline.com
*.las2b.citrixonline.com
*.launch.gotowebinar.com
*.line-apps.com
```

```
[!] SSL Front: app.gotomeeting.com
[!] SSL Front: br.gotomeeting.com
[!] SSL Front: free.gotomeeting.com
[!] SSL Front: get.gotomeeting.com
[!] SSL Front: getstage.gotomeeting.com
[!] SSL Front: no.gotomeeting.com
[!] SSL Front: pl.gotomeeting.com
[!] SSL Front: stage2.gotomeeting.com
[!] SSL Front: stage1.gotomeeting.com
[!] SSL Front: stage3.gotomeeting.com
[!] SSL Front: stage4.gotomeeting.com
[!] SSL Front: stage.gotomeeting.com
[!] SSL Front: www1.gotomeeting.com
[!] SSL Front: www2.gotomeeting.com
[!] SSL Front: www3.gotomeeting.com
[!] SSL Front: www4.gotomeeting.com
[!] SSL Front: www.gotomeeting.com
[!] SSL Front: cdn-matome.line-apps.com
[!] SSL Front: support.logmein.com
[!] SSL Front: advocacy.mozilla.org
[!] SSL Front: archive.mozilla.org
[!] SSL Front: badges.mozilla.org
[!] SSL Front: docs.telemetry.mozilla.org
[!] SSL Front: donate.mozilla.org
[!] SSL Front: ftp.eu.mozilla.org
[!] SSL Front: ftp.mozilla.org
[!] SSL Front: ftp-ssl.mozilla.org
[!] SSL Front: games.mozilla.org
[!] SSL Front: learning.mozilla.org
[!] SSL Front: releases.mozilla.org
[!] SSL Front: riskheatmap.security.mozilla.org
[!] SSL Front: science.mozilla.org
[!] SSL Front: surveillance.mozilla.org
[!] SSL Front: teach.mozilla.org
[!] SSL Front: telemetry.mozilla.org
[!] SSL Front: thimble.mozilla.org
[!] SSL Front: wirelesschallenge.mozilla.org
[!] SSL Front: cdn-static.onepagecrm.com
[!] SSL Front: 11.osding.com
[!] SSL Front: help.periscope.tv
```

<https://github.com/vysec/DomainFrontingLists/blob/master/CloudFront-SSL-PA-Exempt.txt>





E-mail Delivery

Configuring E-mail Security is hard

SPF, DMARC, DKIM

Sender Policy Framework (SPF)

Domain Message Authentication, Reporting and Conformance (DMARC)

DKIM? Forget that for now. Get the basics right first!

SPF is USELESS without DMARC

Many people have told me otherwise
Always turns out to be the same

SPF

Specifies a list of IP addresses and domains who are allowed to send on behalf of your domain.

Consider issues with shared SMTP servers on the cloud!

Get SPF record:

```
nslookup -q=txt domain.com
```

```
v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com  
ip4:147.243.128.24 ip4:147.243.128.26 ip4:147.243.1.153 ip4:147.243.1.47  
ip4:147.243.1.48 -all
```

DMARC

Controls what happens when SPF fails for an e-mail

VERY important.

- No DMARC record? Fail open and allow
- Bad Configuration? Exploitable too!

Get DMARC record:

```
nslookup -q=txt _dmarc.domain.com
```

```
v=DMARC1; p=reject; pct=100; rua=mailto:d@rua.agari.com;  
ruf=mailto:d@ruf.agari.com; fo=1
```

DMARC Policy

p: policy

sp: subdomain policy

Specify a strong policy for both s, and sp.

Values:

- None <- **BAD**
- Quarantine <- Go to JUNK and click on obviously bad e-mails
- Reject <- **GOOD**

v=DMARC1; p=quarantine; sp=quarantine; ruf=mailto:dmARC@domain.com; rf=afrf;
pct=100; ri=86400

Domain vs. Subdomain

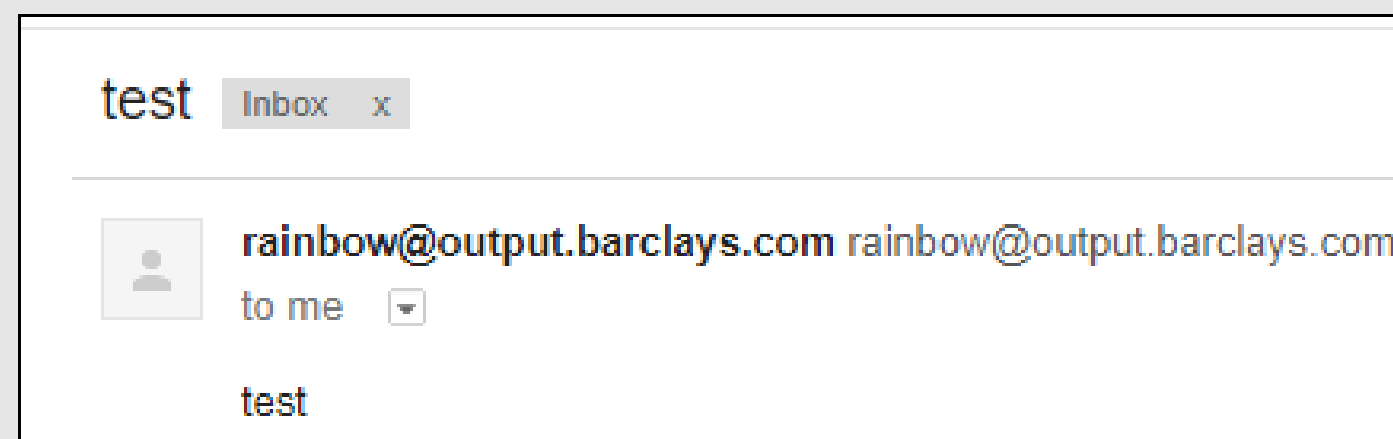
Always protect your subdomains!

Example
Good SPF: 

```
[*] v=spf1 include:spf.messagelabs.com include:servers.mcsv.net ip4:160.34.64.28 include:_spf.salesforce.com ip4:208.185.235.45 ip4:12.70.67.12 ip4:213.200.109.65 ip4:205.217.12.155 ip4:180.87.148.12 ip4:89.187.113.3 include:successfactors.eu include:spf1.barclays.com ip4:216.74.162.17 ip4:216.74.162.18 ip4:94.236.35.193 ip4:193.148.38.199 ip4:217.11.0.38 ~all
```

Bad Subdomain DMARC: 

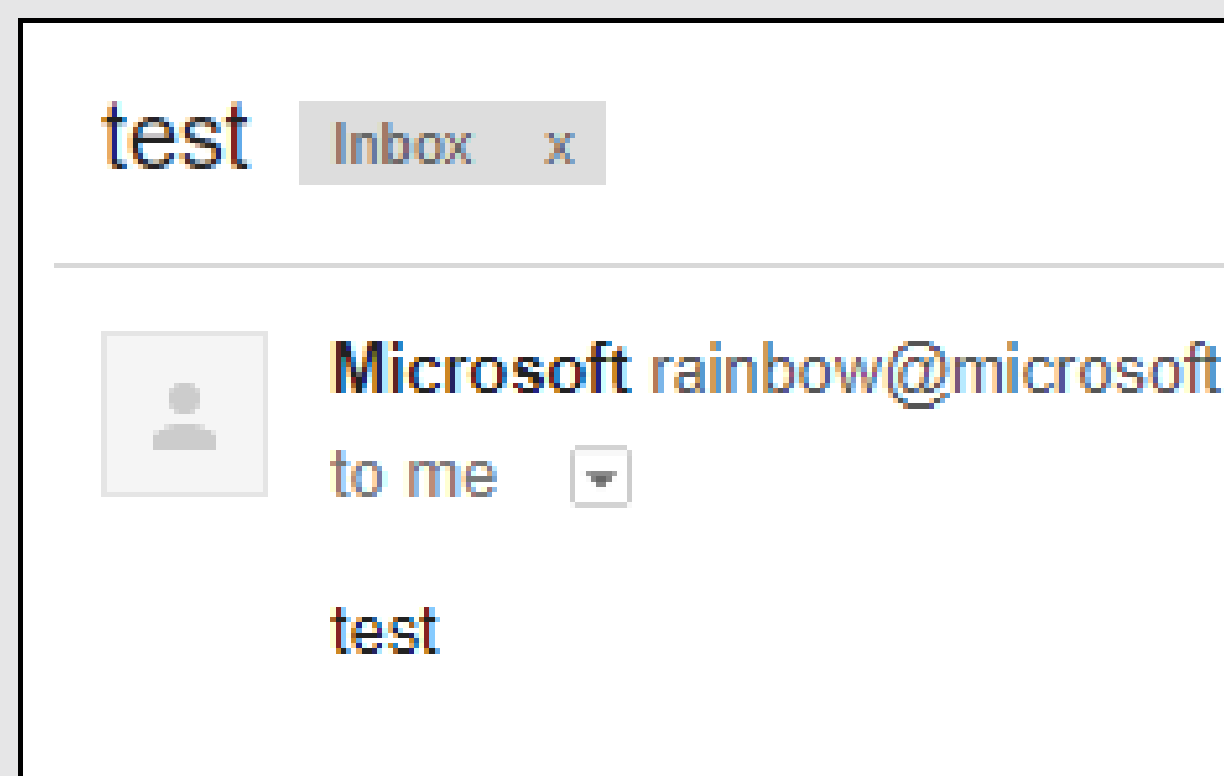
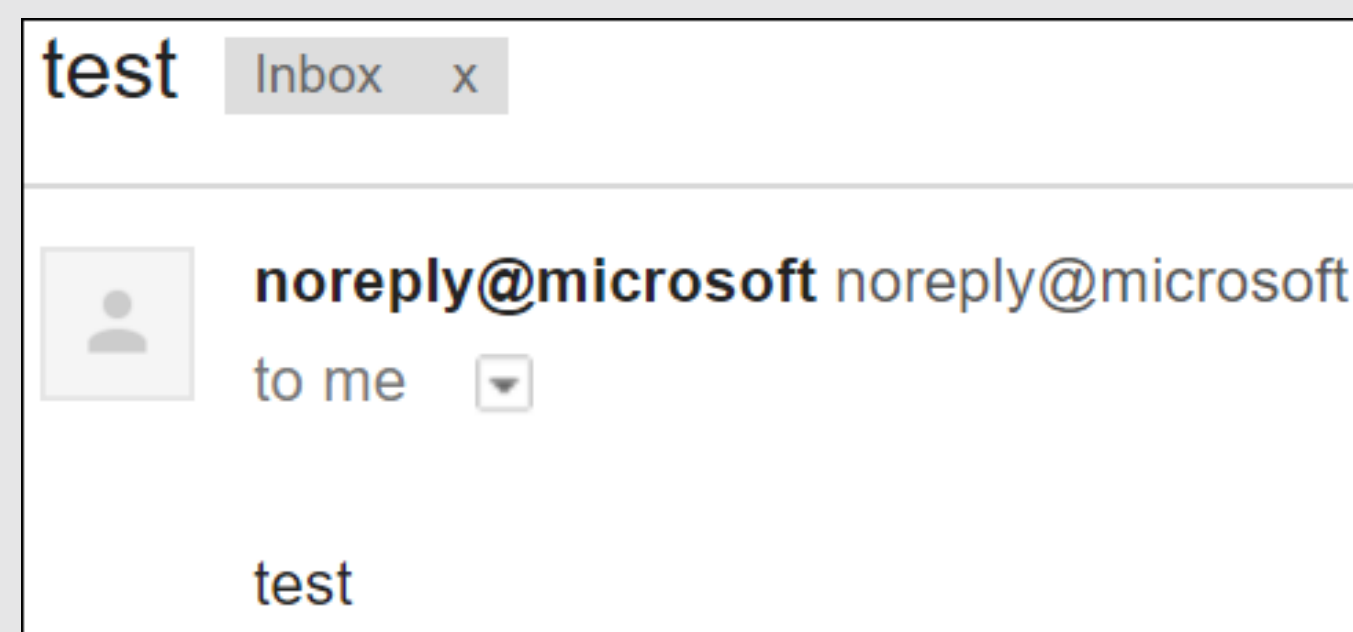
```
v=DMARC1;p=reject;sp=none;fo=1;ri=3600;rua=mailto:barclays@rua.agari.com;ruf=mailto:barclays@ruf.agari.com
```



What if... I use a TLD?

Example

- Can't spoof **Microsoft.com**
- Try to spoof **Microsoft**



Can't set DMARC because don't own the domain
Not too bad

Office365

Popular cloud based e-mail service provider

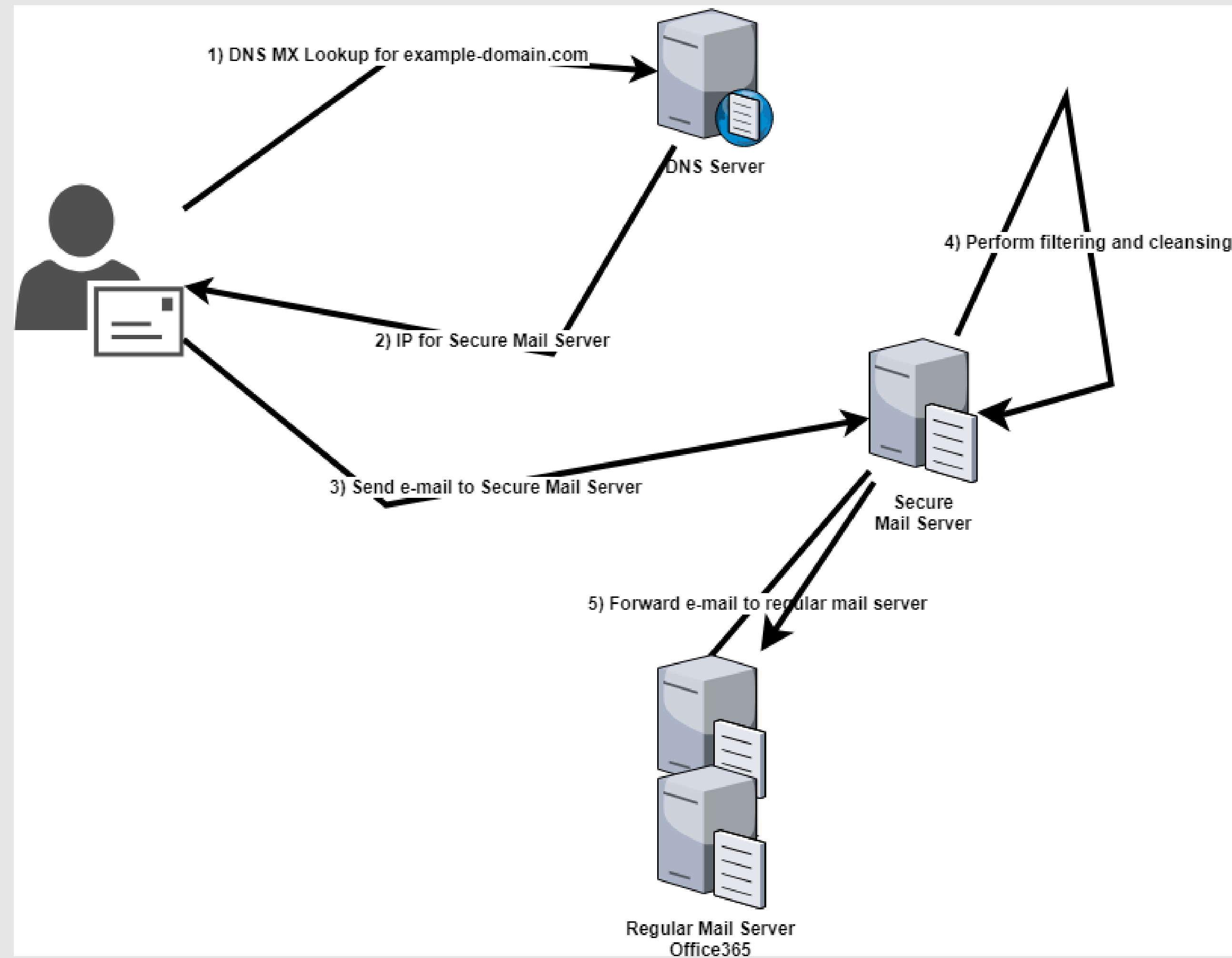
E-mail spoofing issues in Office365

Research by **Jonathan Echavarria** (@und3rf10w)

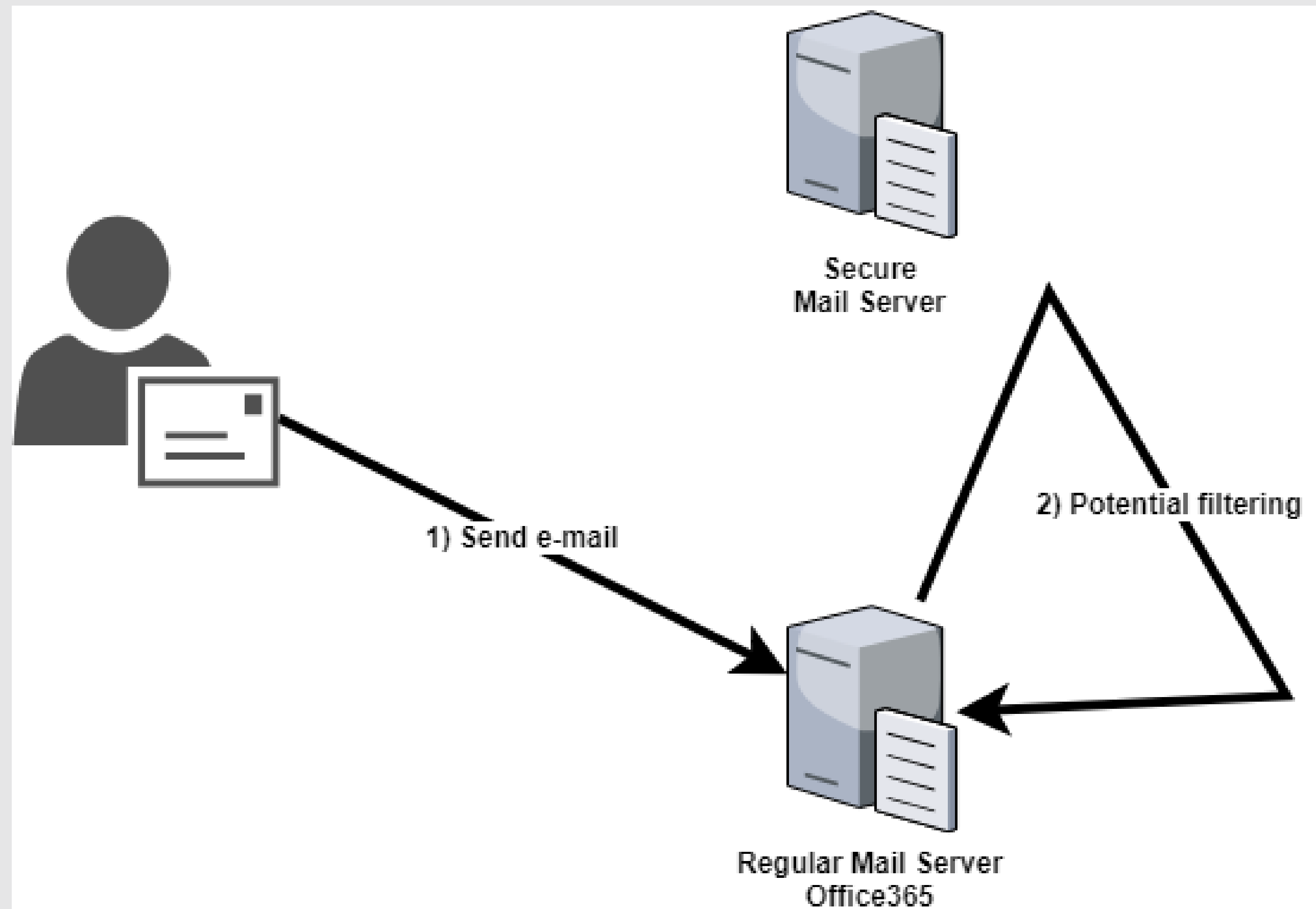
Discusses ProofPoint bypass by accessing 0365 directly

<https://und3rf10w.blogspot.com/2017/07/abusing-misconfigured-cloud-email.html>

Regular E-mail Flow



Und3f10w's Finding



Bypass Additional E-mail Servers

Eg. ProofPoint or Mimecast

Connect directly to the Office365 server

- Bypass spam filters
- Bypass self-spoof filter on ProofPoint

Say goodbye to the security investment!

Does the target use Office365?

Take: `mycompanydomain.com`

Replace all `.` with `-`: `mycompanydomain-com`

Append 0365 server (mail.protection.outlook.com):

`mycompanydomain-com.mail.protection.outlook.com`

DNS lookup:

```
C:\Users\vysec>nslookup [REDACTED].mail.protection.outlook.com
Server:  router.asus.com
Address: 192.168.50.1

Non-authoritative answer:
Name:    [REDACTED].mail.protection.outlook.com
Addresses: 207.46.163.74
           207.46.163.42
```

Other Office365 Regions

China: mycompanydomain-com.mail.protection.partner.outlook.cn

Germany: mycompanydomain-com.mail.protection.outlook.de

<https://github.com/vysec/check0365>



So how does it work?

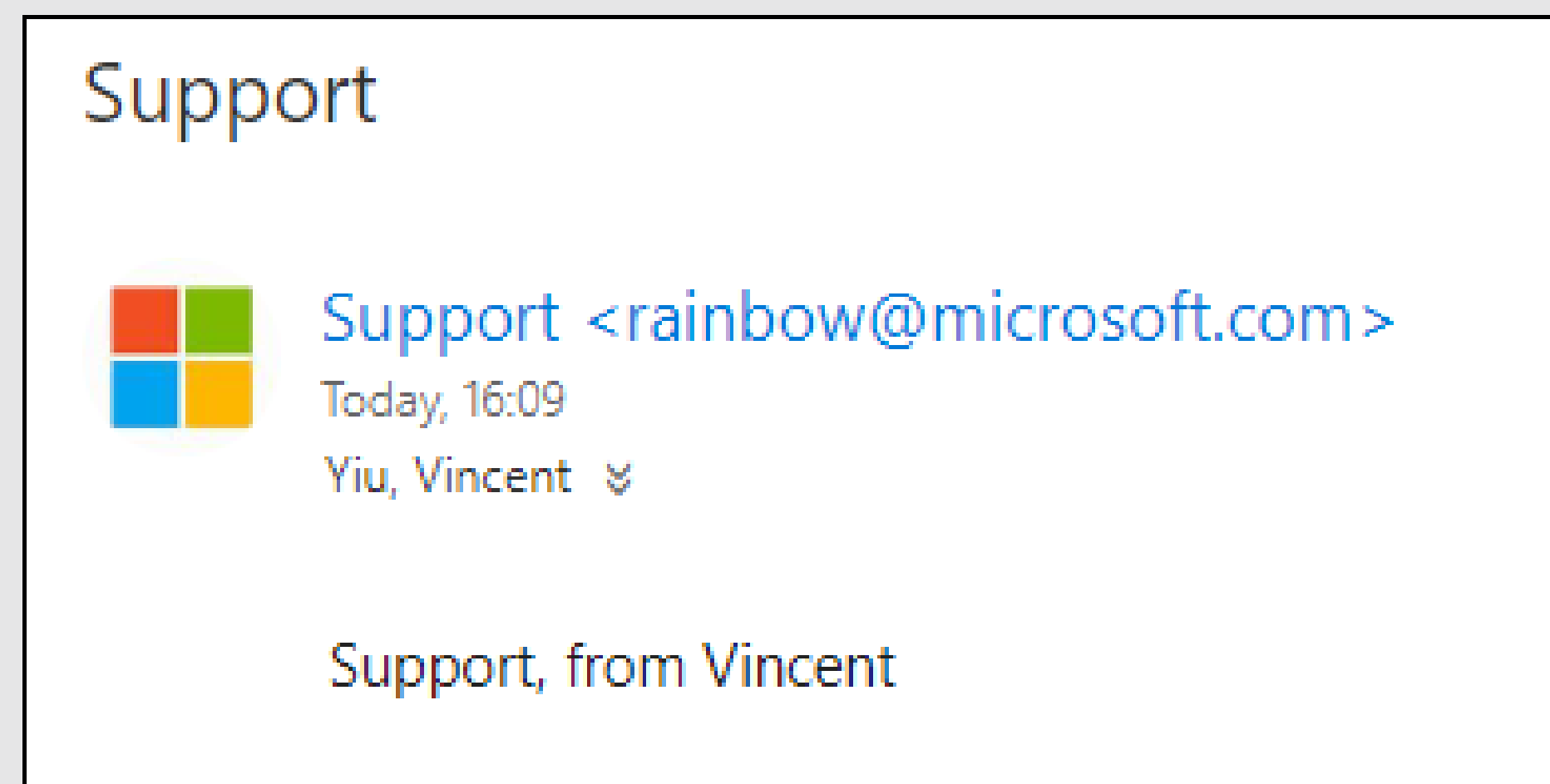
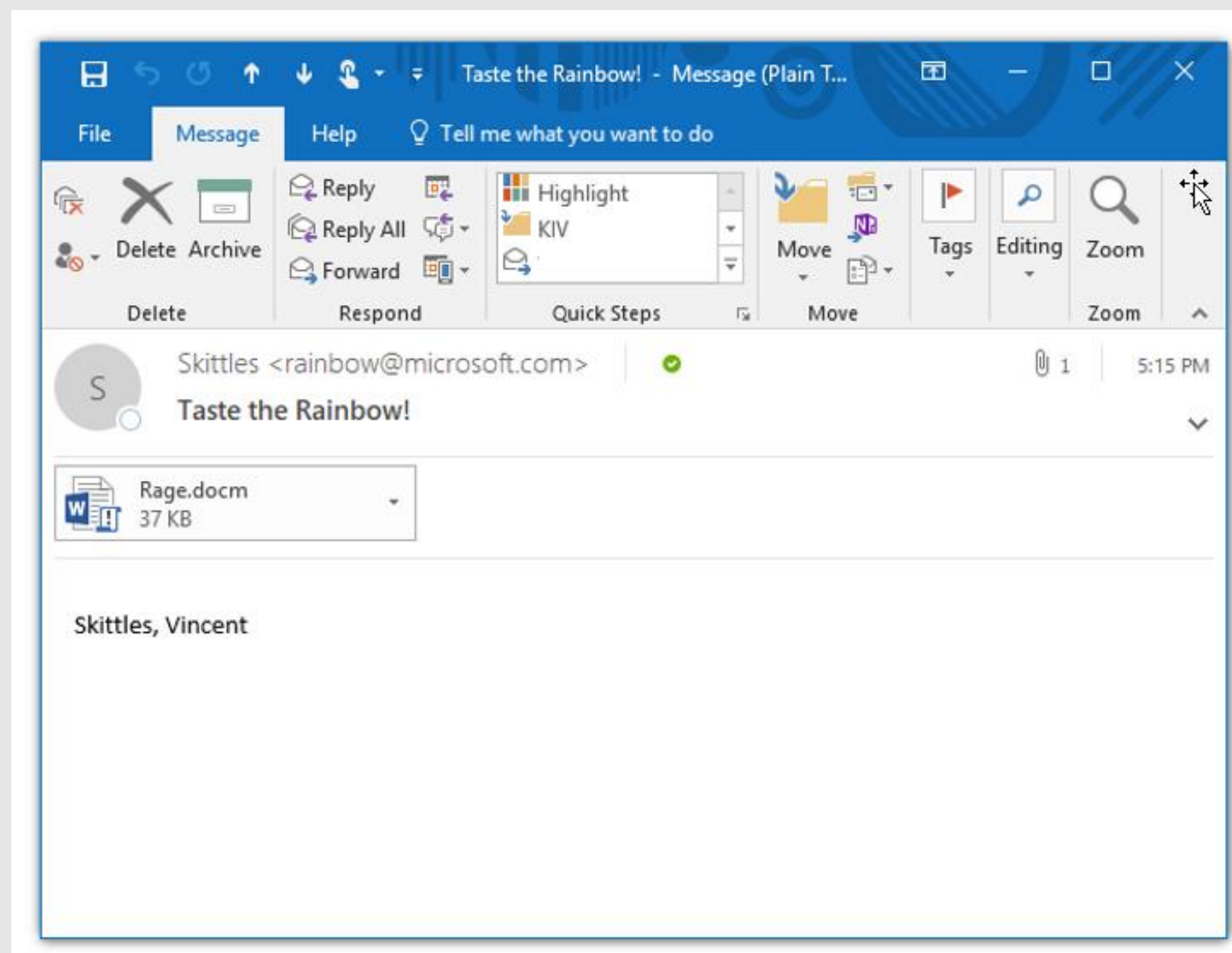
Office365 SMTP Servers do not use authentication

Caveat: can only relay e-mails to Office365 tenants...

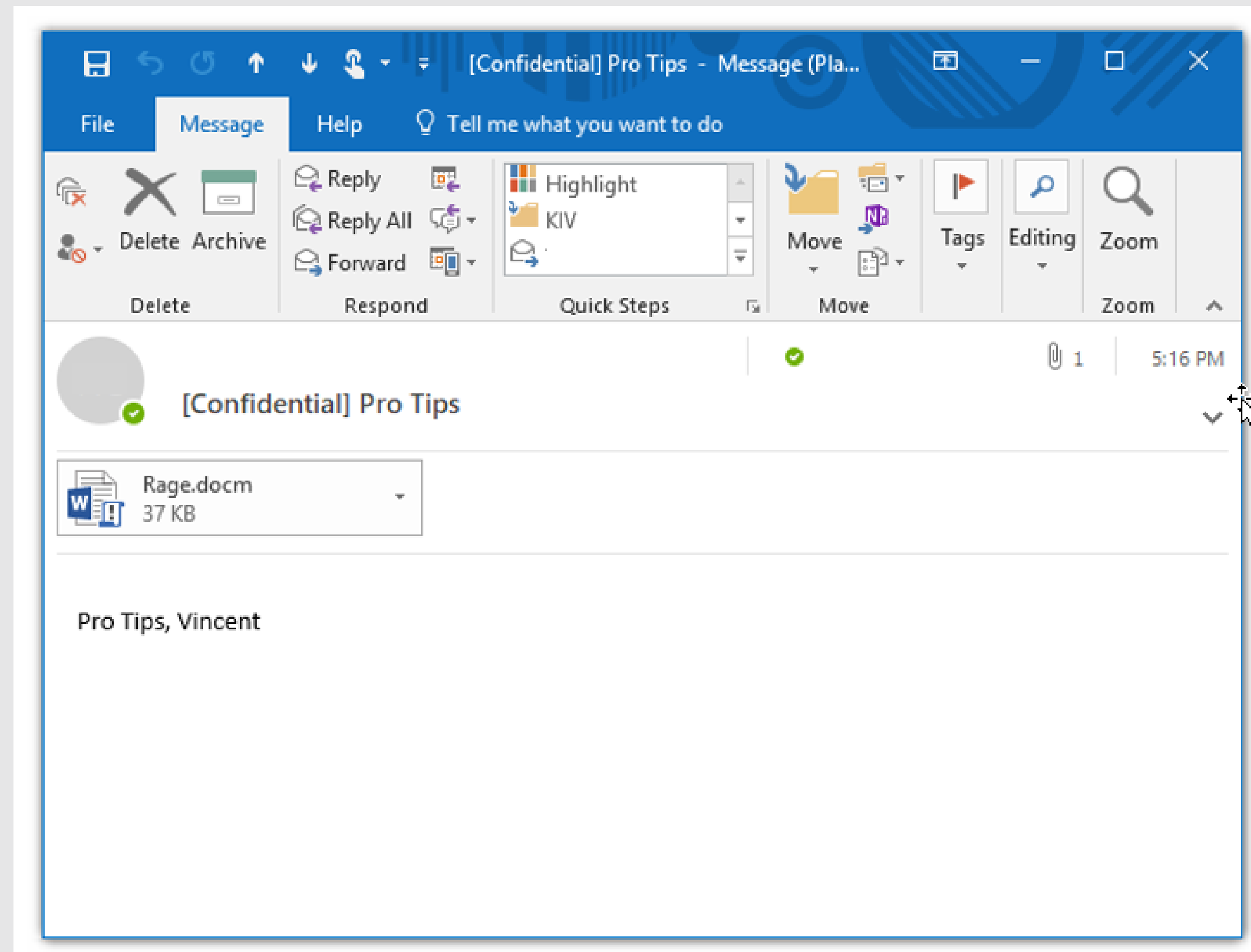
Example exploit:

```
sendmail -f rainbow@microsoft.com  
-t user@tenant.com -u test -m test  
-s <tenant-com.mail.protection.outlook.com>
```


Relay between Tenants



Relay between Regions



TenantInboundAttribution

```
Jun 14 10:31:44 ip-172-31-30-215 sendmail[25247]: WARNING => The recipient ondcolleascolleary@bta.com was rejected by the mail server, error follows:  
Jun 14 10:31:44 ip-172-31-30-215 sendmail[25247]: WARNING => Received: 550 5.7.51 TenantInboundAttribution; There is a partner connector configured that matched the message's recipient domain. The connector had either the RestrictDomainsToIPAddresses or RestrictDomainsToCertificate set [PRODPROTECTPROTECT-PROD.prod.protection.outlook.com]  
Jun 14 10:31:44 ip-172-31-30-215 sendmail[25247]: ERROR => Exiting. No recipients were accepted for delivery by the mail server.
```

RestrictDomainsToIPAddress
RestrictDomainsToCertificate

Bypass TenantInboundAttribution

Use a different Edge Node for a different tenant

Find an insecure edge node to use as a relay SMTP server

<https://github.com/vysec/Office365TenantsList>

Example exploit:

```
sendemail -f rainbow@microsoft.com  
-t user@tenant.com -u test -m test  
-s <other-tenant.mail.protection.outlook.com>
```

Issues

Office365 has a SPAM filter

Recently having issues spoofing @microsoft.com

URLs in e-mails with TLDs such as .host, .space are flagged as SPAM

Always test the spoofing per engagement

Microsoft making changes really quick

Questions?

vincentyiou.co.uk



Twitter: @vysecurity



WeChat:

