

**WE CAN**

**WIPE**

**YOUR EMAIL**

# WHO WE ARE?



**ILYA NESTEROV**

Security researcher

I break things

I build things to break things



**MAX GONCHAROV**

Security researcher

Threat OSINT

Vulnerability hunter

# WHY EMAIL?

Hillary Clinton was asked if she wiped the disc she was using for her email; she said, 'Do you mean with a damp cloth?' This, to me, is frightening. John McAfee





# HILLARY CLINTON

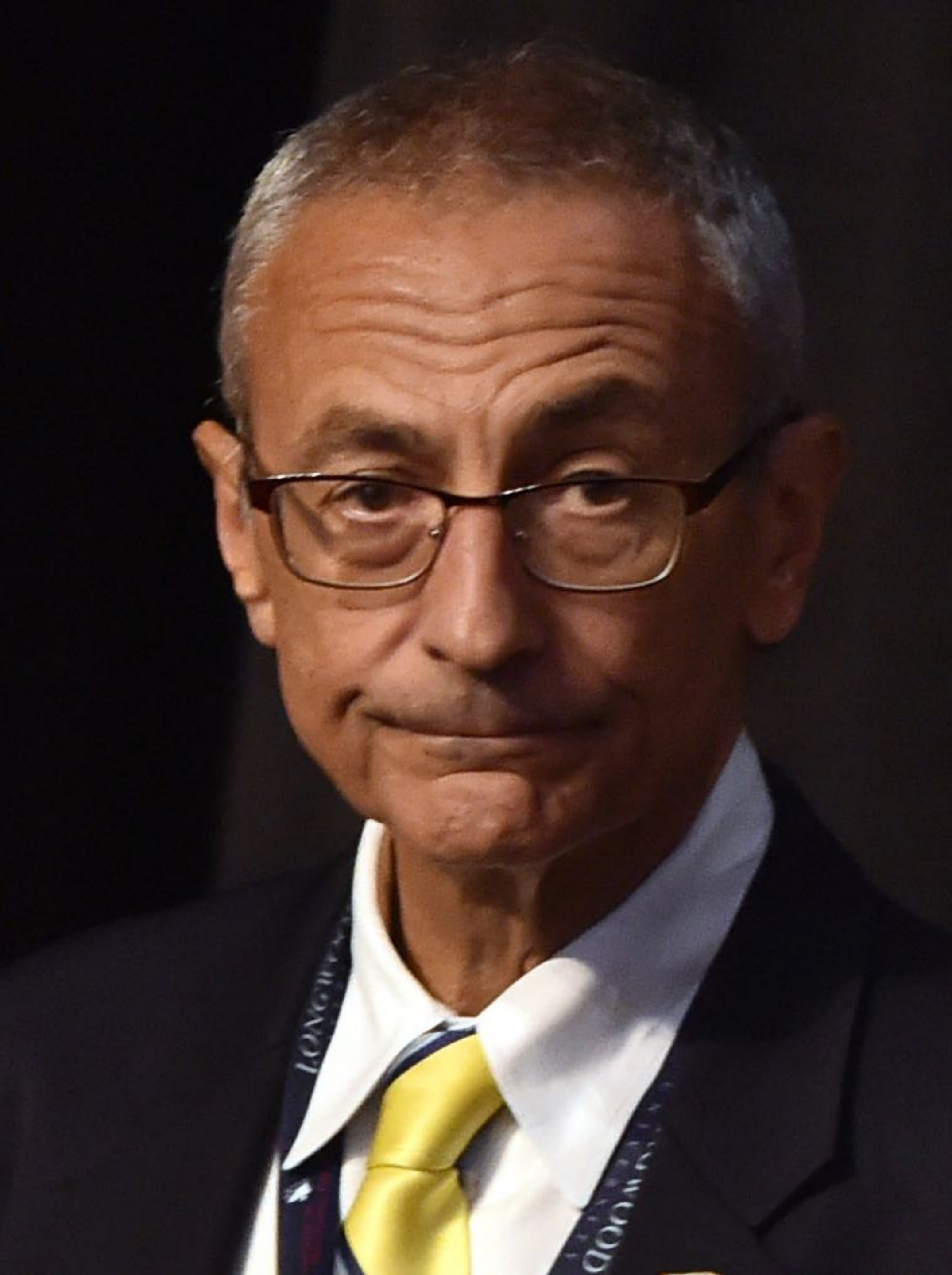
---

**26260** EMAILS

**53** PEOPLE

JUN 2010 TO DEC 2014





# JOHN PODESTA

---

**34500** EMAILS

**287** PEOPLE

FEB 2006 TO DEC 2016





# DNC

---

**19252** EMAILS

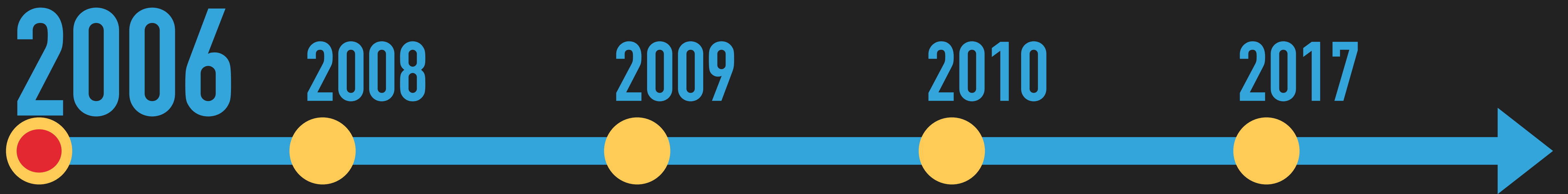
**1586** PEOPLE

OCT 2013 TO MAY 2016



# PASSIVE ATTACKS ON EMAIL CLIENTS

# AUTODISCOVER : HISTORY

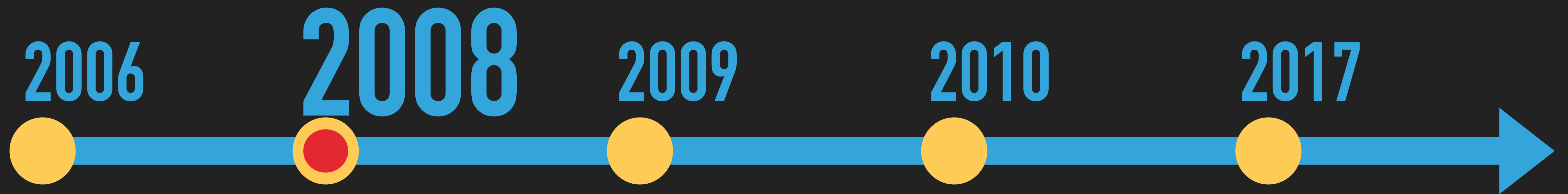


## FEATURE FOR OFFICE 2007

- ▶ AUTODISCOVER ANNOUNCED AS A FEATURE FOR THE UPCOMING PRODUCT RELEASE



# AUTODISCOVER : HISTORY



## INTRODUCED

APRIL 2008

- ▶ INTRODUCED AS VERSION 0.1 WITH PRELIMINARY DESCRIPTION OF THE SERVICE.

# AUTODISCOVER : HISTORY

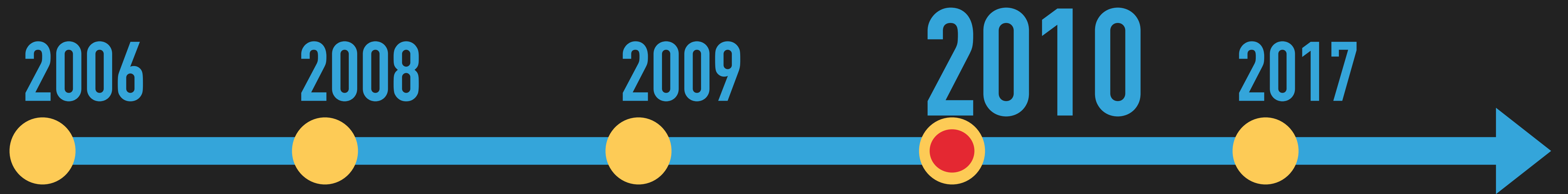


## THUNDERBIRD CONFIG-V1.1.XML

- ▶ ALTERNATIVE OF AUTODISCOVER FOR THUNDERBIRD PROPOSED IN 2008 AND RELEASED IN 2009.



# AUTODISCOVER : HISTORY



## LYNC SERVER SKYPE FOR BUSINESS

- ▶ PART OF MOBILITY PROGRAM FOR EASIER DATA EXCHANGE. INTRODUCED HTTP AND HTTPS AUTODISCOVER PROCESS

# AUTODISCOVER : HISTORY

2006

2008

2009

2010

2017





# AUTODISCOVER : HISTORY

2006

2008

2009

2010

2017



## NOW WE TALKING AUTODISCOVER MEDNESS

- ▶ WE FOUND SEVERE VULNERABILITIES IN SOME AUTODISCOVER CLIENT IMPLEMENTATIONS.



# AUTODISCOVER : TECH

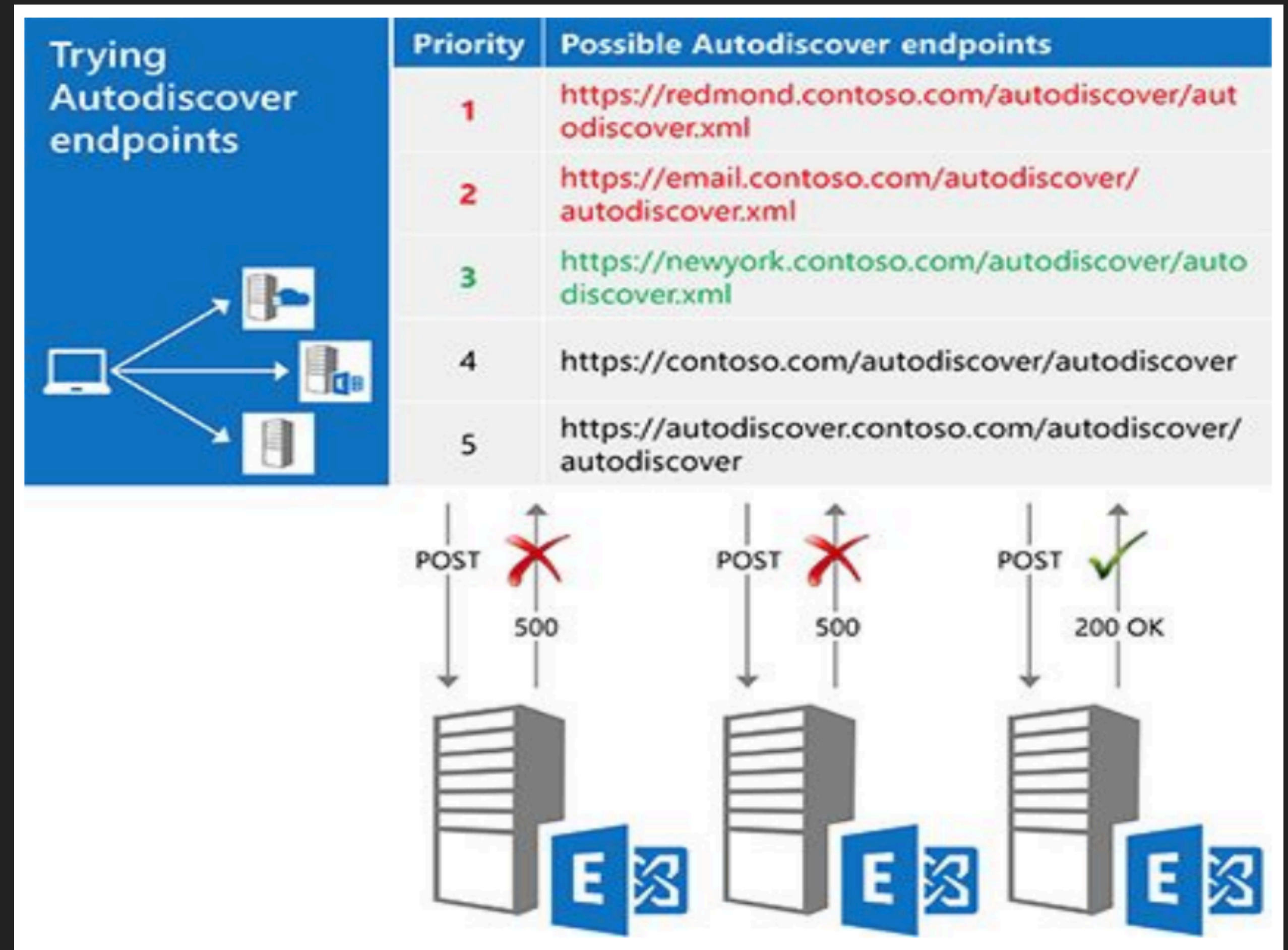
DEFINE THE CANDIDATE POOL



TRY EACH SERVER FROM A LIST

# AUTODISCOVER : TECH

1. QUERY LDAP OR AD SERVERS
2. DERIVE URL FROM THE EMAIL ADDRESS
3. QUERY DNS FOR AUTODISCOVER SRV RECORDS
4. SEND AN UNAUTHENTICATED GET REQUEST
5. PRIORITISE



# AUTODISCOVER : TECH

tomknopf77@jarzt.com



jarzt.com

1. <https://+ {domain} + /autodiscover/autodiscover.xml>
2. <https://autodiscover. + {domain} + /autodiscover/autodiscover.xml>



1. <https://jarzt.com /autodiscover/autodiscover.xml>
2. <https://autodiscover.jarzt.com/autodiscover/autodiscover.xml>



# AUTODISCOVER : TECH

local@domain

tomknopf77@jarzt.com



Local: tomknopf77

Domain: jarzt.com



# AUTODISCOVER : TECH

RFC 5321

RFC 5322

RFC 6531

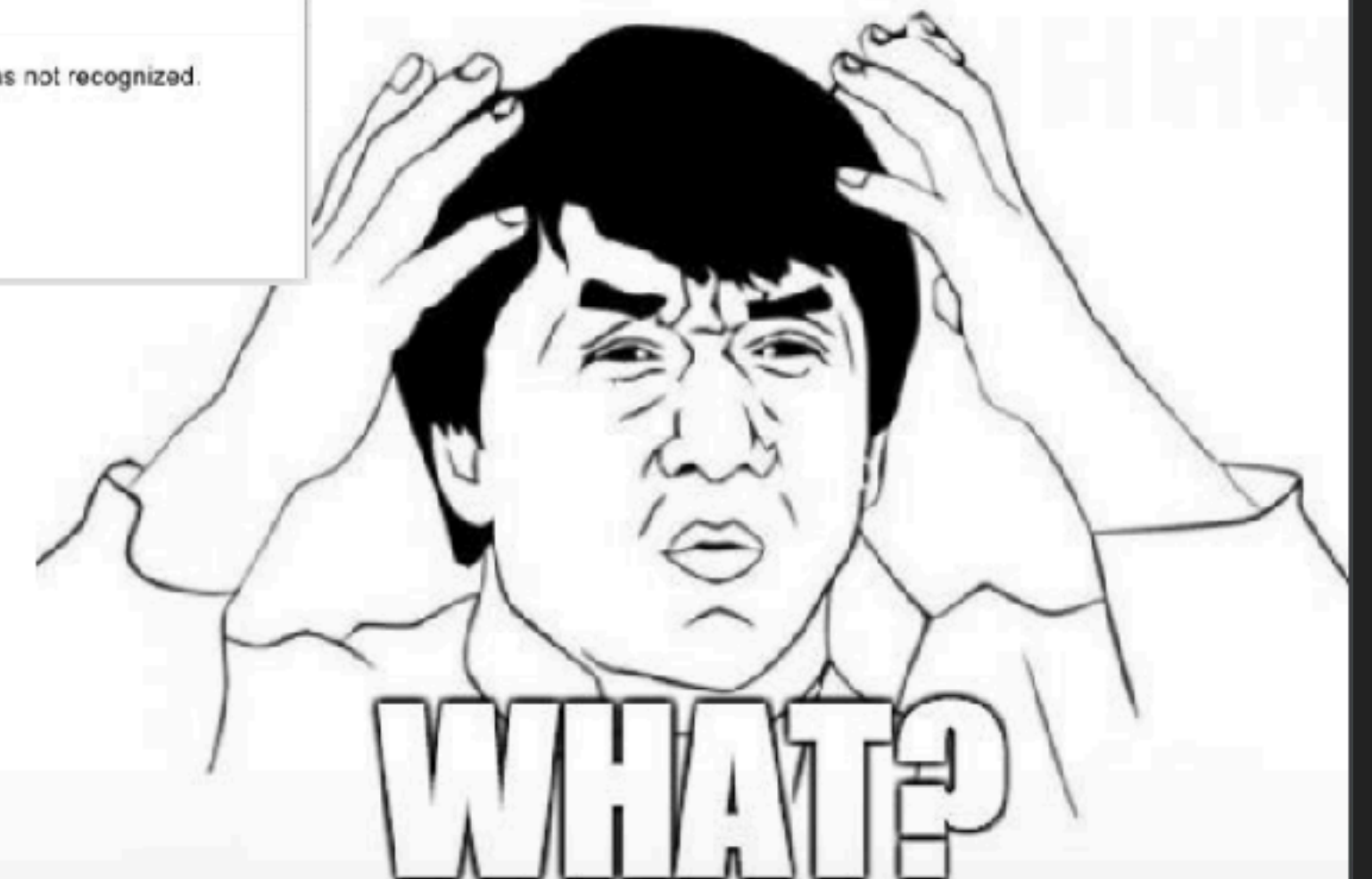
RFC 6532

✓ "()<>[:;,;@\\\\"!#\$%&'-/=?^\_`{| ~.a"@example.org

✗ tom@knopf77@jarzt.com



✓ "tom@knopf77"@jarzt.com





# AUTODISCOVER : TECH

**CVE-2016-9940**



tomknopf77@example.com.au



autodiscover.example.com.au



autodiscover.com.au

**Announced as fixed: January 2017**



# AUTODISCOVER : TECH

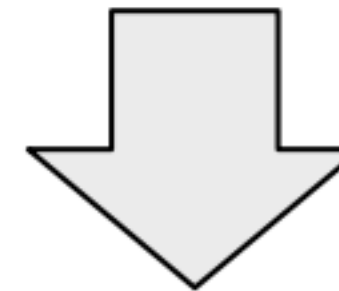
**CVE-2017-2414**



**X** tomknopf77@**example**@com

1 2

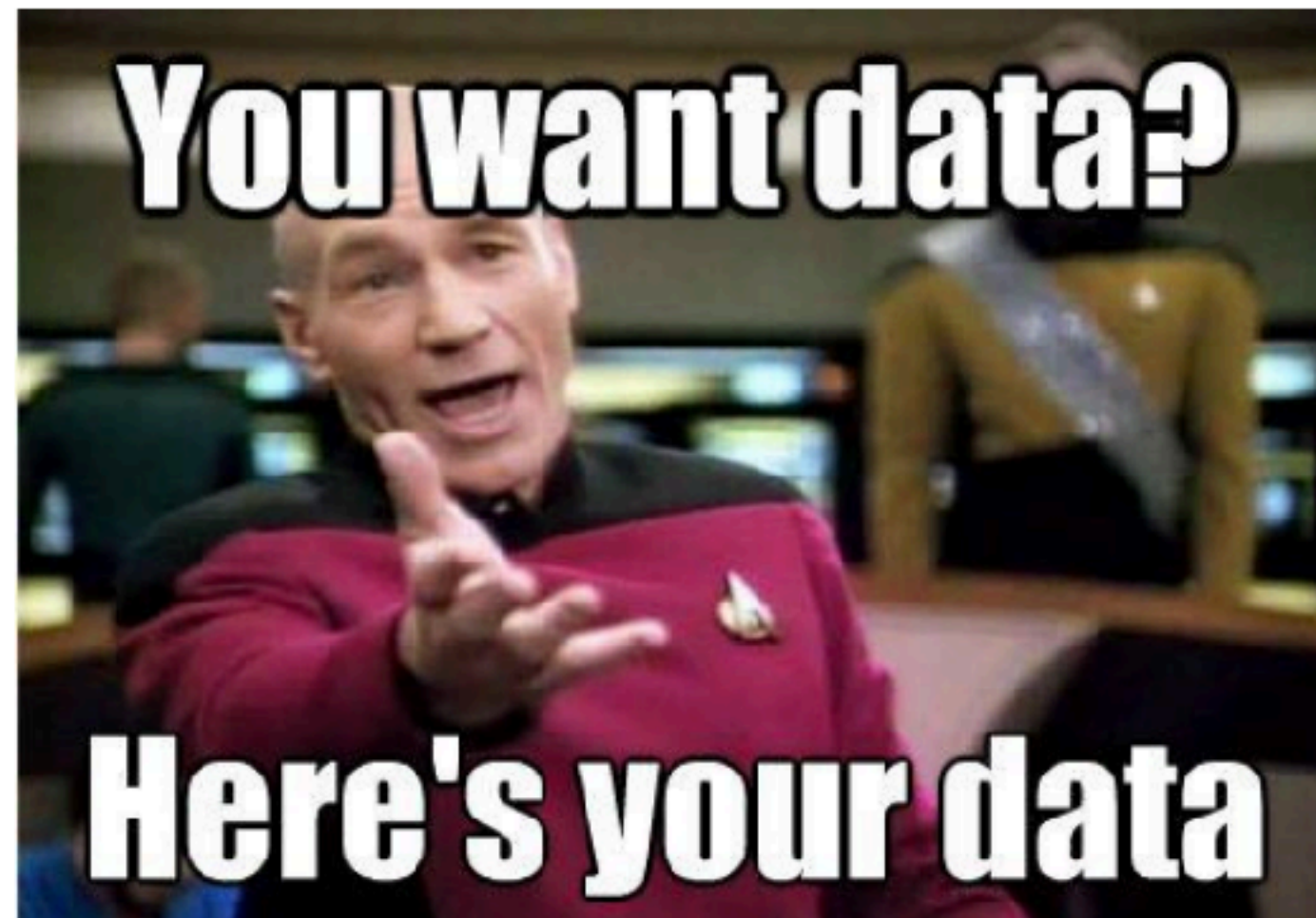
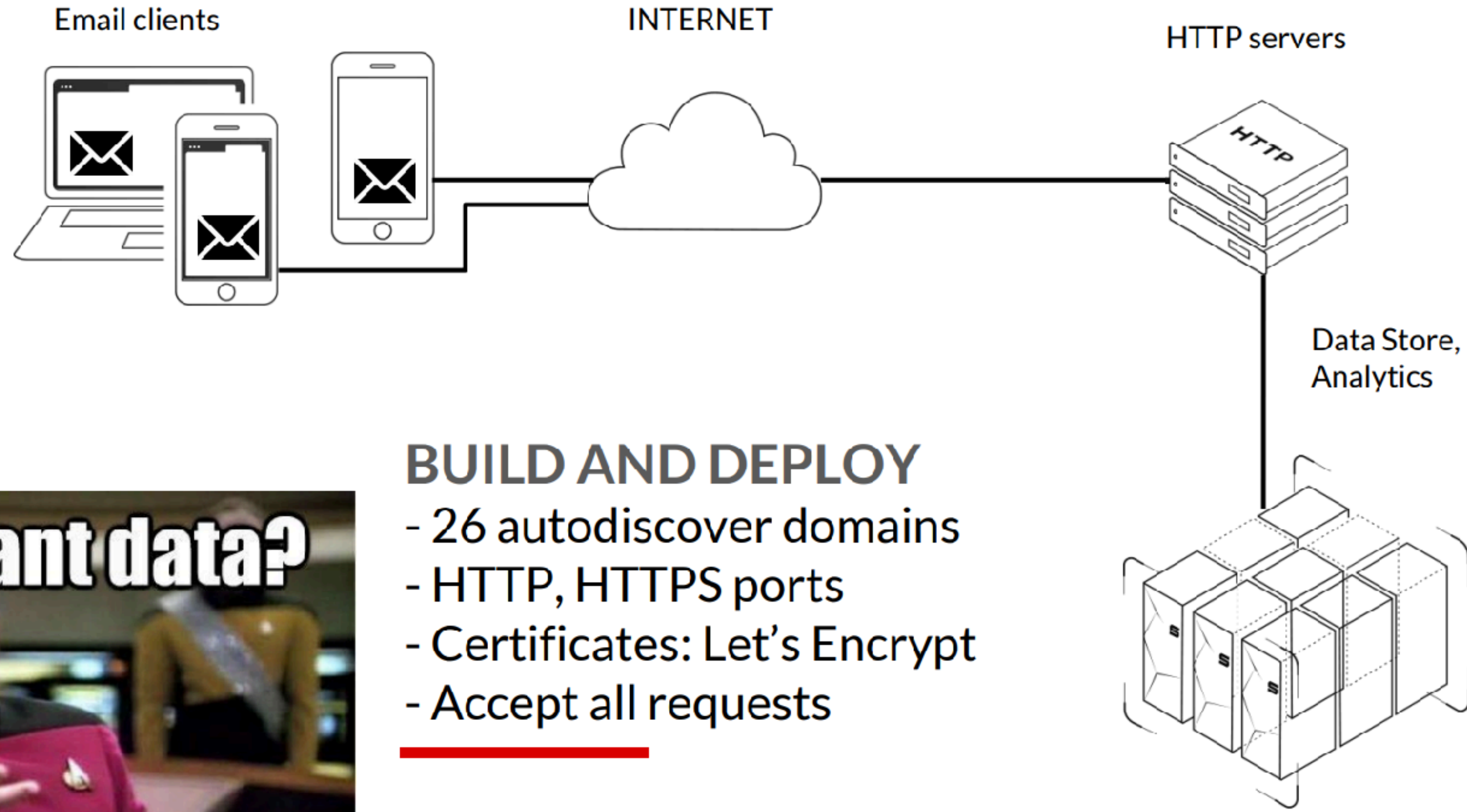
autodiscover. + <domain>



**autodiscover.com**

**Announced as fixed: March 2017. iOS 10.3**

# AUTODISCOVER : TECH



## BUILD AND DEPLOY

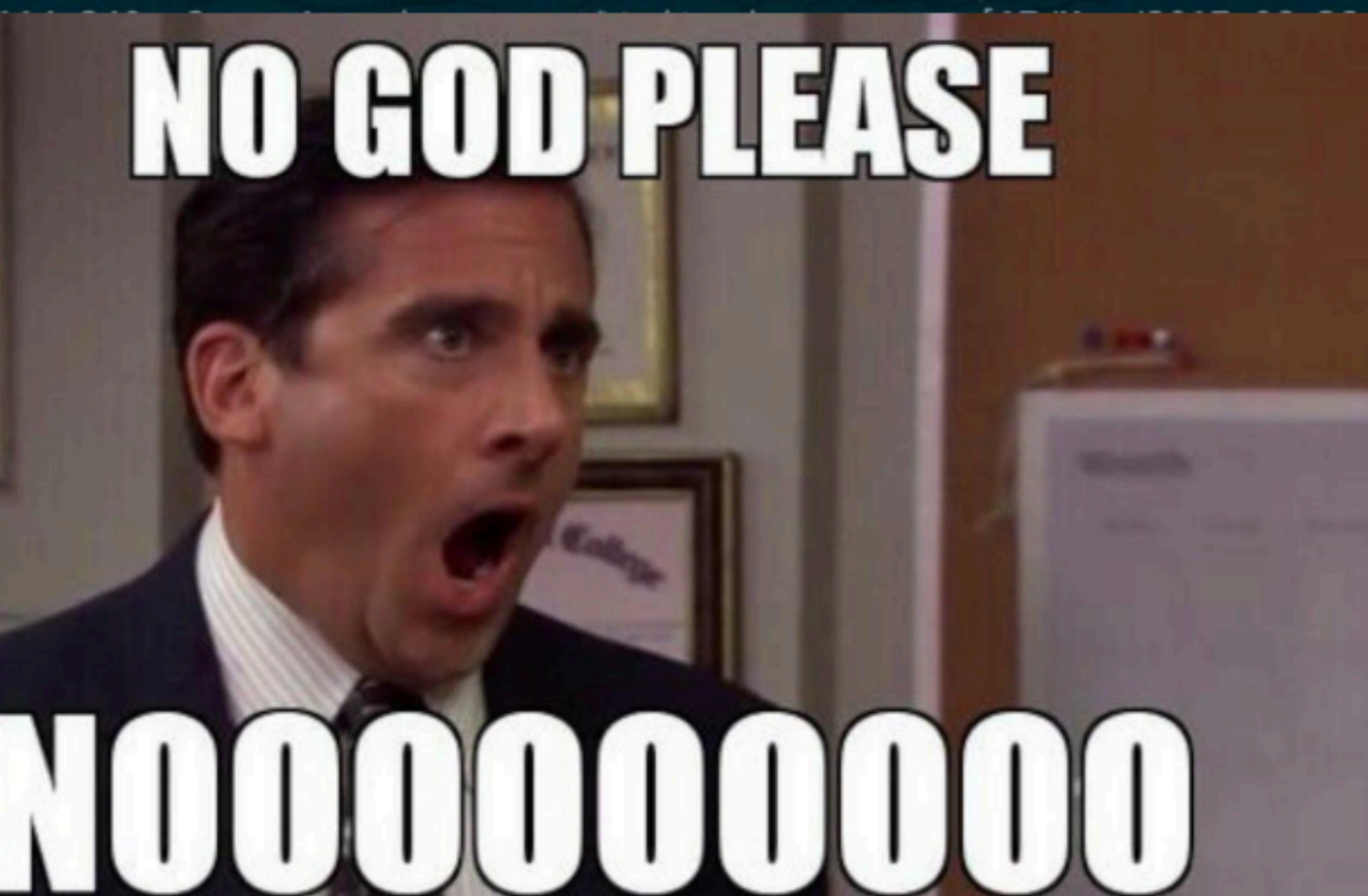
- 26 autodiscover domains
  - HTTP, HTTPS ports
  - Certificates: Let's Encrypt
  - Accept all requests
- 

\* It's just a simple HTTP sink



```
223.104.50 1 - h y@cr [17/Mar/2017:06:26:18 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9008V/101.500" "-"
82.132.2 1 - na Jali@a: [17/Mar/2017:06:26:18 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-GT-S6310N/100.40
114.240. 5 - s @ci: [17/Mar/2017:06:26:19 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9006/101
92.18.1 1 - Da P. k@s: [17/Mar/2017:06:26:19 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-SM-G350/101.40202"
82.132.2 1 - just @a: [17/Mar/2017:06:26:20 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-GT-S6310N/100.4016
223.104. 1 - @i: [17/Mar/2017:06:26:20 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G9008V/101.500
175.223. 1 - h .n@: [17/Mar/2017:06:26:20 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G930K/101.60001"
223.62.7 12 - a 1@ku: [17/Mar/2017:06:26:26 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-T580/101.6000
42.35.1 5 - h @ha: [17/Mar/2017:06:26:26 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G906L/101.60001" "-"
114.240. 5 - s @ci: [17/Mar/2017:06:26:30 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9006/101
85.255. 1 - P @l: [17/Mar/2017:06:26:30 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N91
223.104. 1 - l @i: [17/Mar/2017:06:26:31 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G9008V/101.500
185.69. 1 - A @r: [17/Mar/2017:06:26:31 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N91
86.186. 1 - j @s: [17/Mar/2017:06:26:35 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G900F/101.6
85.255. 1 - v @e: [17/Mar/2017:06:26:35 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910
85.255. 1 - M @e: [17/Mar/2017:06:26:36 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N
148.252. 10 - @w@no: [17/Mar/2017:06:26:41 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9
85.255. 3 - @d@nc: [17/Mar/2017:06:26:43 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/
223.104. 1 - @i: [17/Mar/2017:06:26:44 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G9008V/101.500
79.74. 1 - t @e@ac: [17/Mar/2017:06:26:44 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-GT-P5210/101.40402" "-"
185.69. 1 - / @y: [17/Mar/2017:06:26:47 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N
42.35.1 5 - @h: [17/Mar/2017:06:26:48 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G906L/101.60001" "-"
148.252. 1 - @s@r: [17/Mar/2017:06:26:48 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N
49 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9006/101
6:26:50 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910
017:06:26:51 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM
6:26:52 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910
:06:26:53 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9
6:26:54 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-GT-S6310N/100.4
+0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G900F/101.6
000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G9008V/101.500
000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.6000
"POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G920F/101.50101"
000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G925F/101.6000
:06:27:01 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9
6:27:01 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910
:06:27:03 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9
000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G9008V/101.500
6:27:08 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910
ST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G906L/101.60001" "-"
"POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G930K/101.60001"
06:27:13 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N91
:14 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9005/101
```

**NO GOD PLEASE**



**NOOOOOOOOO**



# PASSIVE ATTACK RESULTS

**22M**

REQUESTS RECEIVED

**18M**

REQUESTS WITH BASIC  
AUTHENTICATION HEADERS

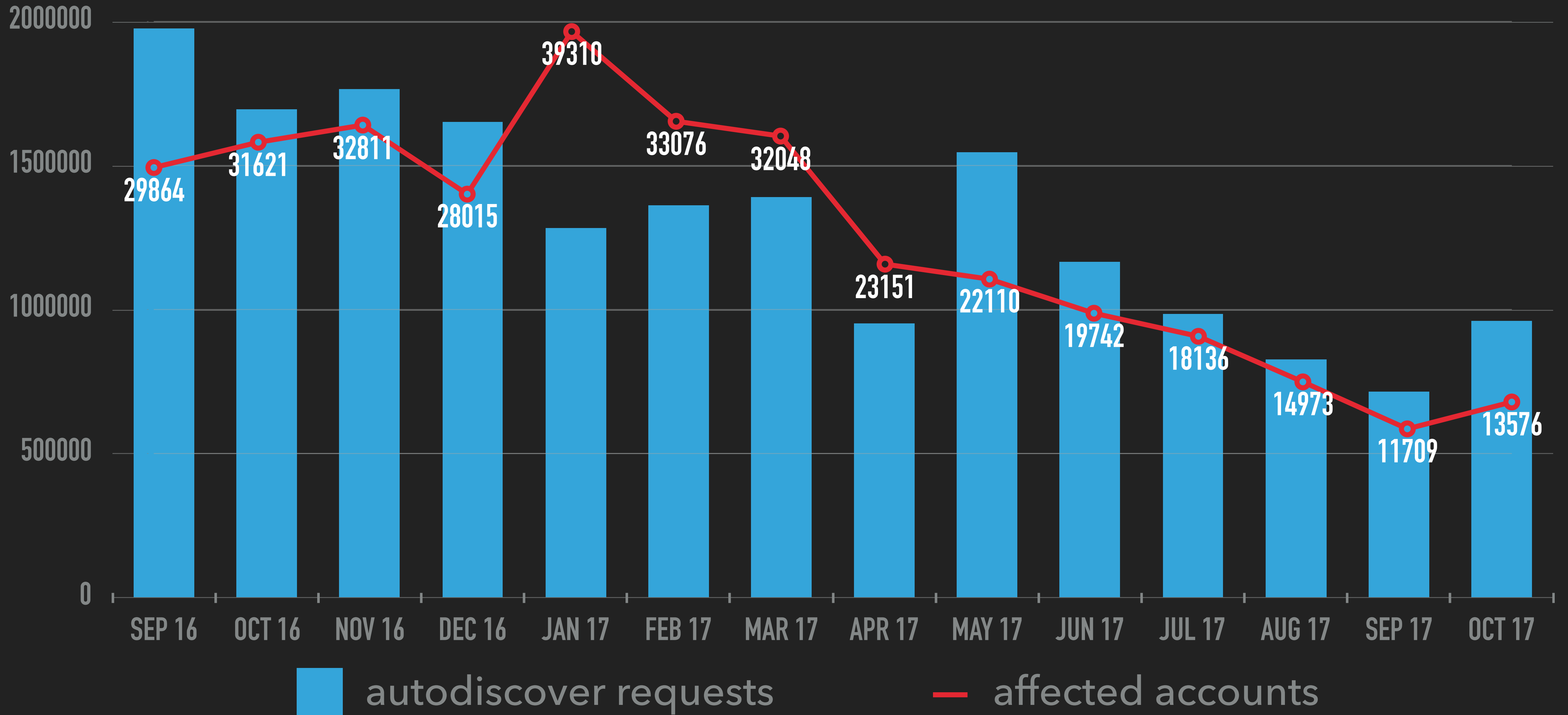
**353K**

EMAIL ACCOUNTS AFFECTED

we need to come up with a better  
name

SEPTEMBER 16 TO OCTOBER 17

# TRENDS





# ACTIVE ATTACKS ON EMAIL CLIENTS



# MOTIVATION

---

DOMAIN REGISTRATION

TARGET SPECIFIC PERSON

AUTODISCOVER PROTOCOL

ONE KEY TO EVERYTHING

EMAIL PROXY

HARD TO DETECT





# WHAT TO ATTACK

---

CLIENT REFRESH CONFIGURATION  
PERIODICALLY

FALLBACK TO INSECURE PROTOCOLS:

GET REQUEST TO **HTTP**

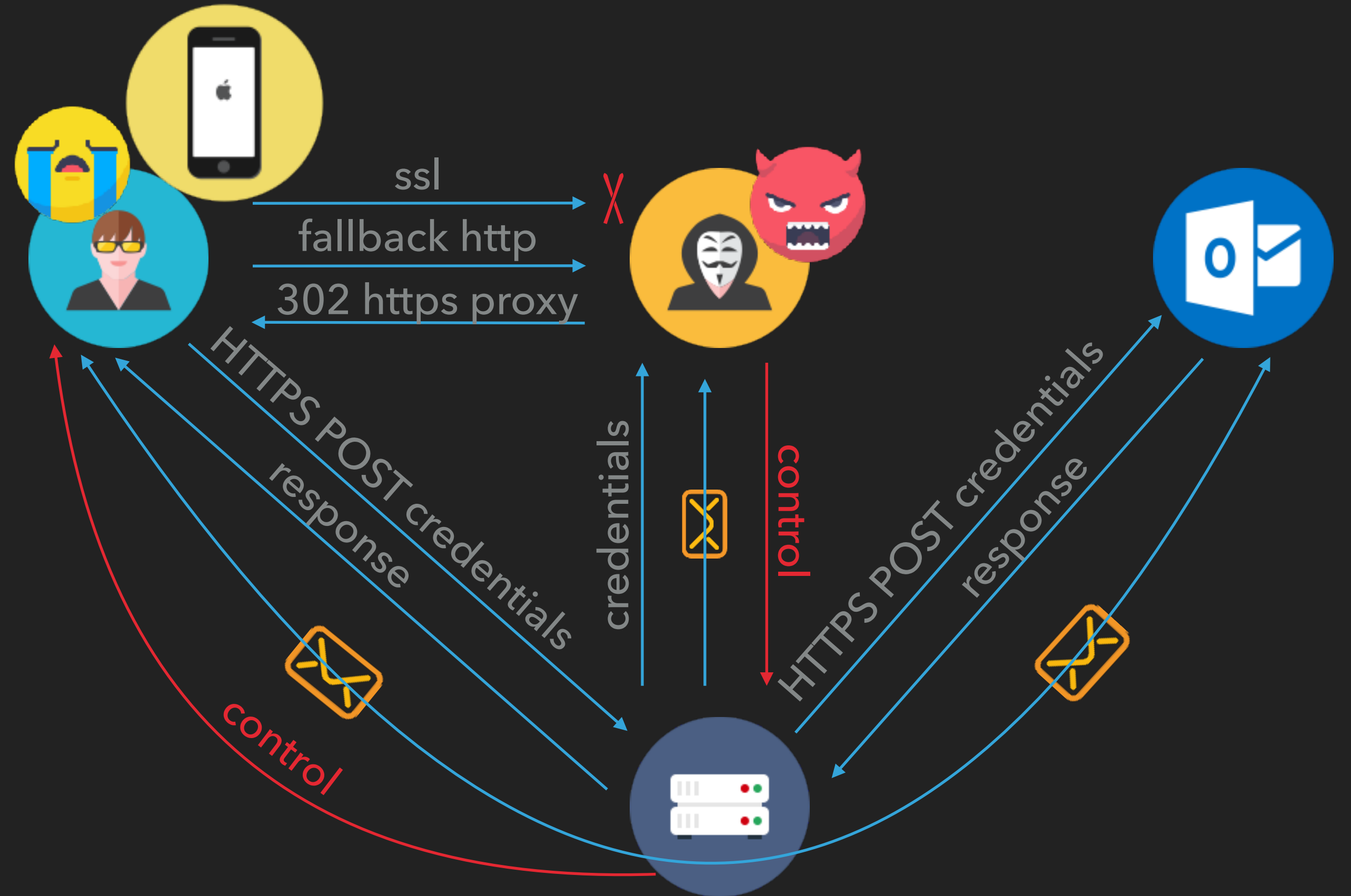
**DNS QUERY**

LET'S MITM!





# NOW WHAT?





# RESULTS

**CVE-2017-7088**: ILYA NESTEROV, MAXIM GONCHAROV



## Exchange ActiveSync

Available for: iPhone 5s and later, iPad Air and later, and iPod touch 6th generation

Impact: An attacker in a privileged network position may be able to erase a device during Exchange account setup ← WTF???

Description: A validation issue existed in AutoDiscover V1. This was addressed by requiring TLS for AutoDiscover V1. AutoDiscover V2 is now supported.

# DISCLOSURE TIMELINE





# WAIT FOR IT

A screenshot of a web browser displaying an Apple Support article. The browser's address bar shows the URL 'https://support.apple.com/en-us/HT208136'. The article title is 'If you can't send an email with iOS 11 and an Outlook.com or Exchange mail account', with a 'Published Date: Sep 26, 2017' tag. The main text explains that users might not be able to send email with Outlook.com, Office 365, or Exchange accounts until they update to iOS 11.0.1. It also describes an error message: 'Cannot Send Mail. The message was rejected by the server.' The article is attributed to Aaron Brown and includes publication and update dates: 'PUBLISHED: 08:21, Fri, Sep 22, 2017 | UPDATED: 08:21, Fri, Sep 22, 2017'.

Apple Inc. [US] | <https://support.apple.com/en-us/HT208136>

Published Date: Sep 26, 2017

## If you can't send an email with iOS 11 and an Outlook.com or Exchange mail account

You might not be able to send email with an Outlook.com, Office 365, or Exchange account until you update to iOS 11.0.1.

If your email account is hosted by Microsoft on [Outlook.com](https://outlook.com) or Office 365, or an Exchange Server 2016 running on Windows Server 2016, you might see this error message when you try to send an email with iOS 11: "Cannot Send Mail. The message was rejected by the server."

of new features to iPhone and iPad owners. However, some users should stay well away from the new iOS upgrade, and this is why.

By **AARON BROWN**  
PUBLISHED: [08:21, Fri, Sep 22, 2017](#) | UPDATED: 08:21, Fri, Sep 22, 2017



I'm actually thinking to put demo before the slide with an explanation (slide 11 "Now what") and change that slide name to smtp like Wait.. How?



# DEMO TIME





# METHODOLOGY

---

- ▶ CHECK RESISTANCE TO MITM:
  - ▶ DO NOT TRUST INVALID CERTIFICATE
  - ▶ DO NOT CACHE INVALID CERTIFICATE
- ▶ AUTODISCOVER PROTOCOL ISSUES:
  - ▶ AUTODISCOVER URL IS PROPERLY DERIVED
  - ▶ TLD, PUBLIC SUFFIX USAGE
  - ▶ NO HTTP
  - ▶ SHOULDN'T BLINDLY SEND CREDENTIALS





# RESULTS

---

5 TOP IOS AND ANDROID EMAIL APPS:





# WHY IT IS A PROBLEM

---

**8K+** MOZILLA PUBLIC SUFFIX LIST

**1.5K+** IANA TLD LIST

PEOPLE MAKE MISTAKES:

USER@CO

USER@COM.CO

**0** CLIENTS WARN USER

FALLBACK TO INSECURE PROTOCOLS

NO WAY FOR CERTIFICATE PINNING



# WHAT CAN WE DO ABOUT IT?

## USERS/ENTERPRISE

USE RECOMMENDED CLIENTS

STAY UP TO DATE

EMAIL ENCRYPTION

ZERO TRUST (FORCE VPN, TLS)

TEST YOUR EMAIL CLIENTS

## SOFTWARE DEVELOPERS

DO NOT USE HTTP

FOLLOW BEST PRACTICES

WARN ABOUT TLD AND  
PUBLIC SUFFIX

TRUST BUT VERIFY

SAML, OAUTH, MFA





Questions  
**Answers**