
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?

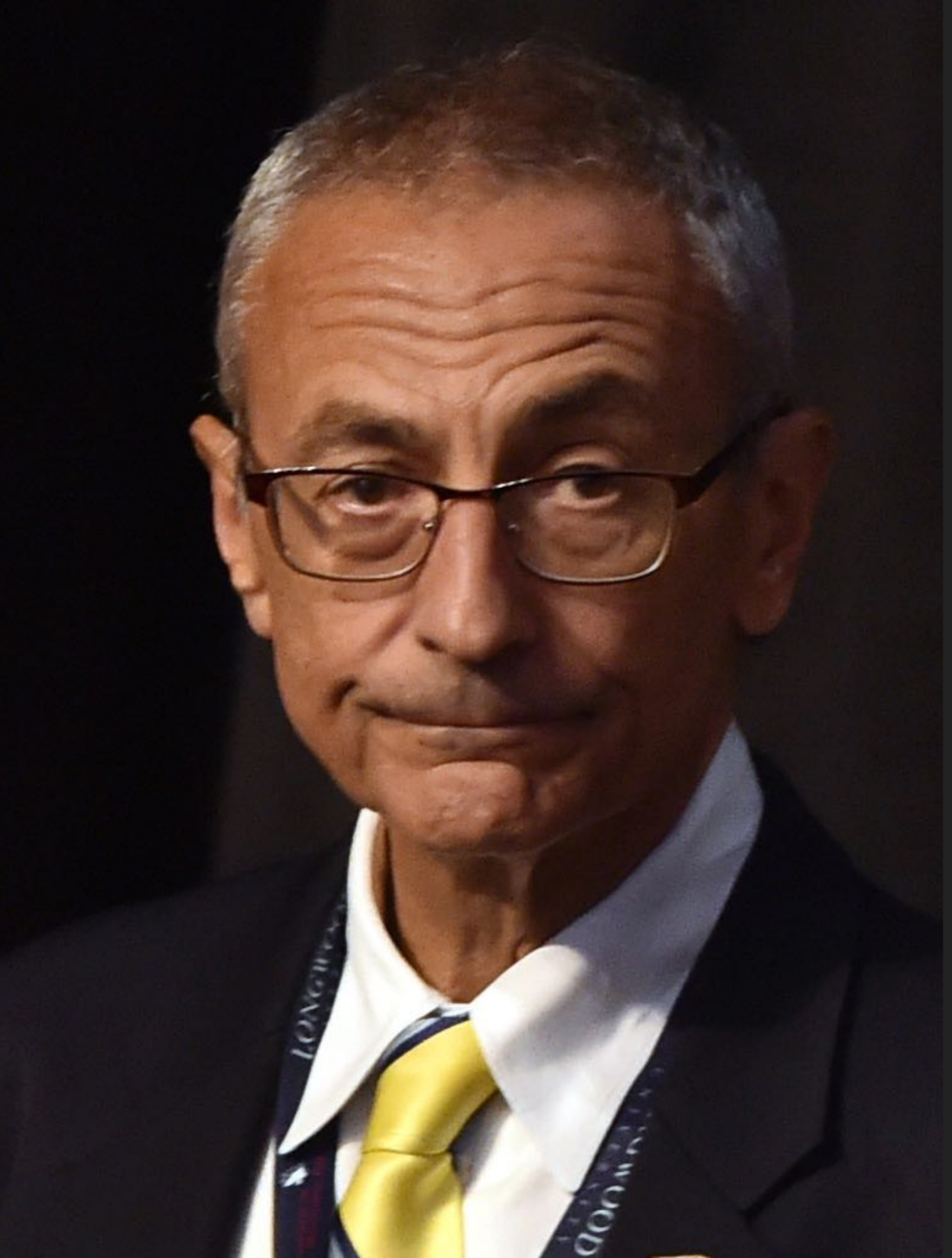
Hillary Clinton was asked if she wiped the disc she was using for her email; she said, 'Do you mean with a damp cloth?' This, to me, is frightening. John McAfee

HILLARY CLINTON

26260 EMAILS

53 PEOPLE

JUN 2010 TO DEC 2014



JOHN PODESTA

34500 EMAILS

287 PEOPLE

FEB 2006 TO DEC 2016

DNC

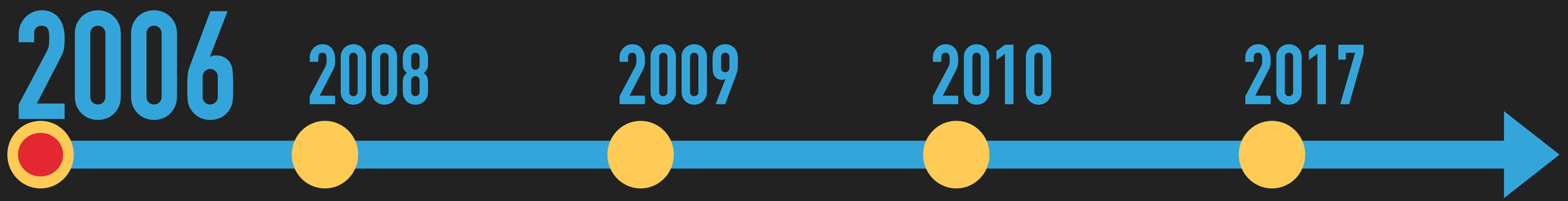
19252 EMAILS

1586 PEOPLE

OCT 2013 TO MAY 2016

PASSIVE ATTACKS ON EMAIL CLIENTS

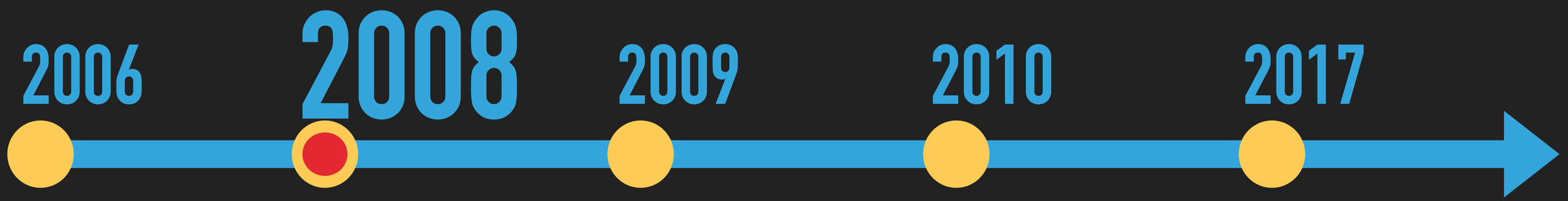
AUTODISCOVER : HISTORY



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.

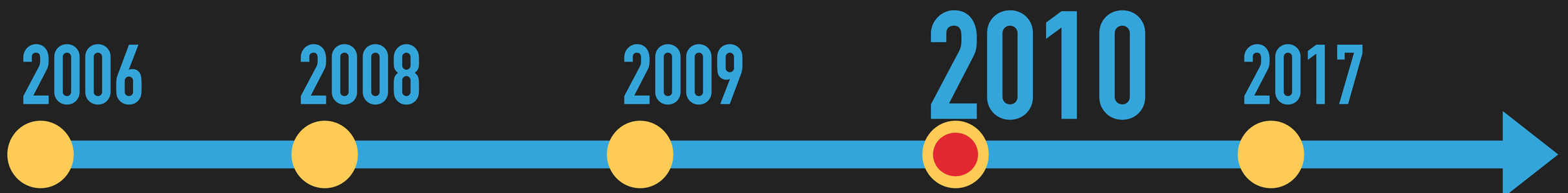
AUTODISCOVER : HISTORY

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

With Autodiscover We found severe vulnerabilities in some autodiscover client implementations.

NOW WE TALKING

AUTODISCOVER MEDNESS

- WE FOUND SEVERE VULNERABILITIES IN SOME AUTODISCOVER CLIENT IMPLEMENTATIONS.

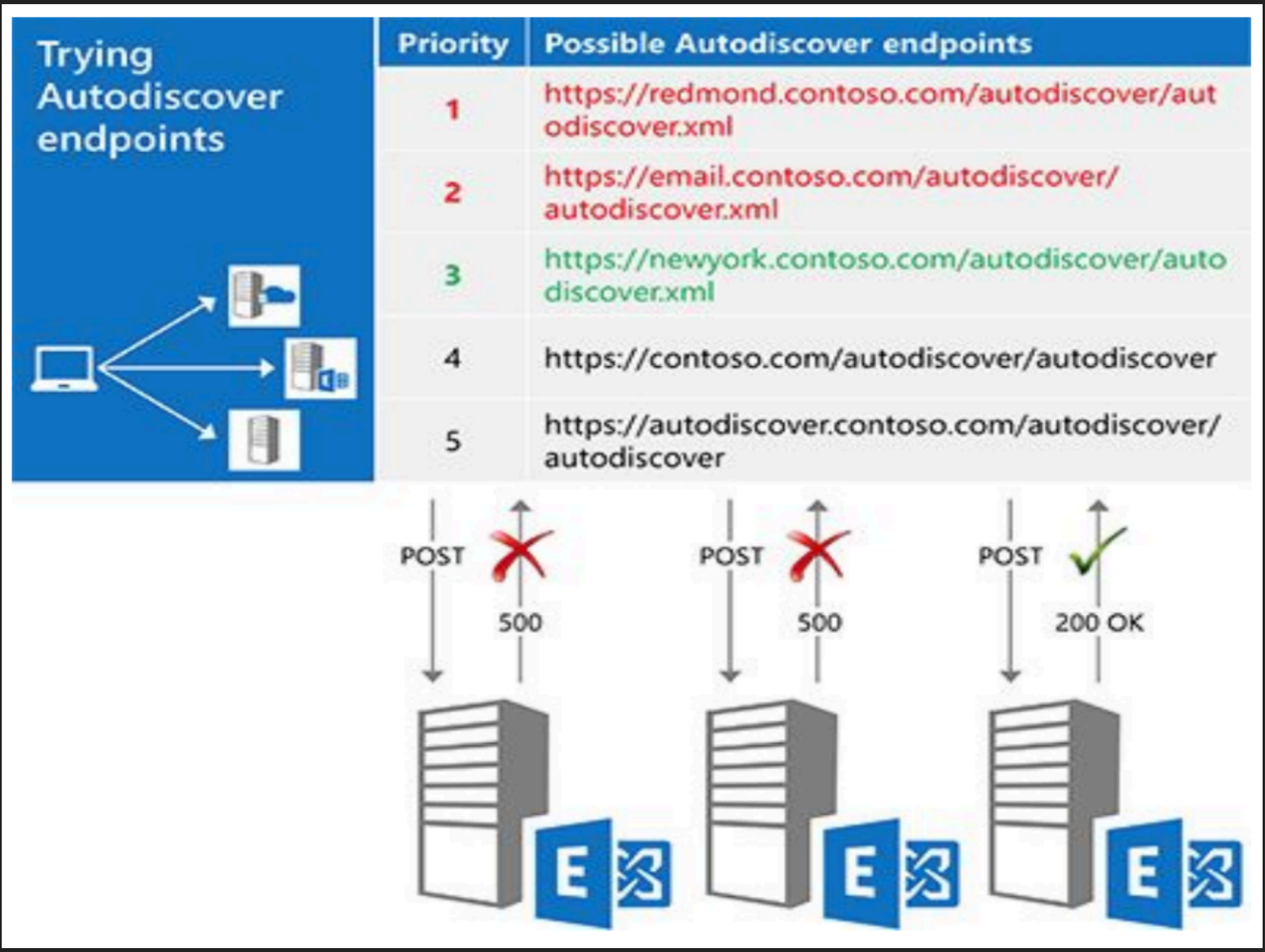
AUTODISCOVER : TECH

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

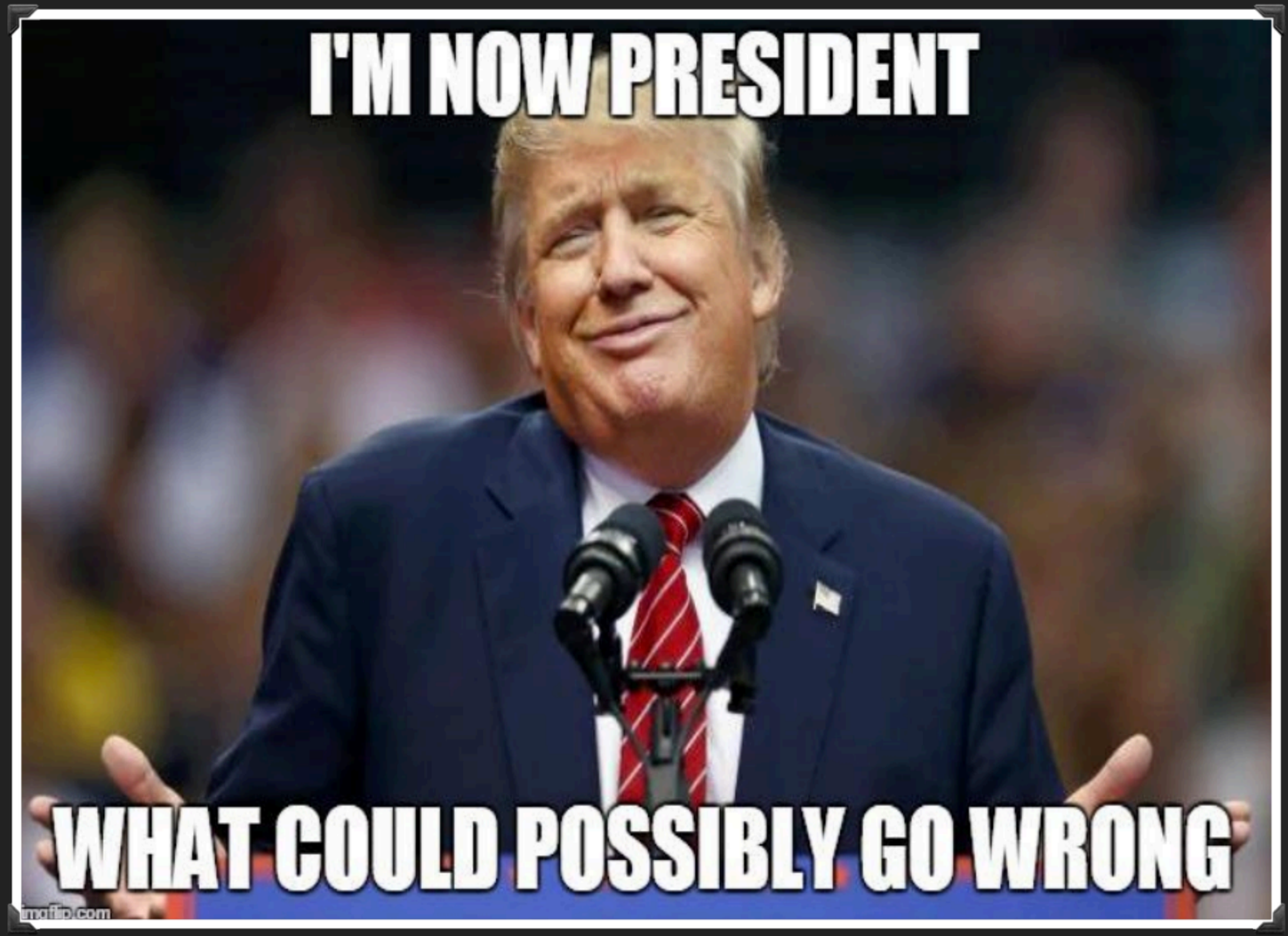
AUTODISCOVER : TECH

local@domain

tomknopf77@jarzt.com

Local: tomknopf77

Domain: jarzt.com



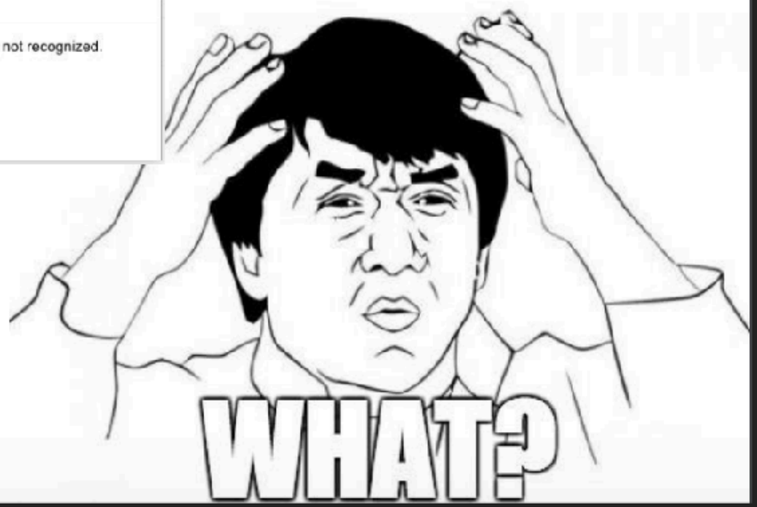
AUTODISCOVER : TECH

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

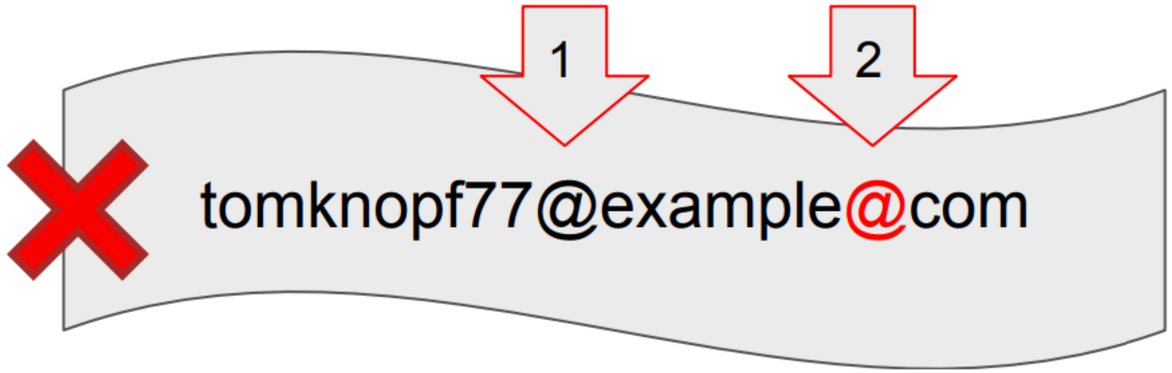
✓ autodiscover.example.com.au

✗ autodiscover.com.au

Announced as fixed: January 2017

AUTODISCOVER : TECH

CVE-2017-2414

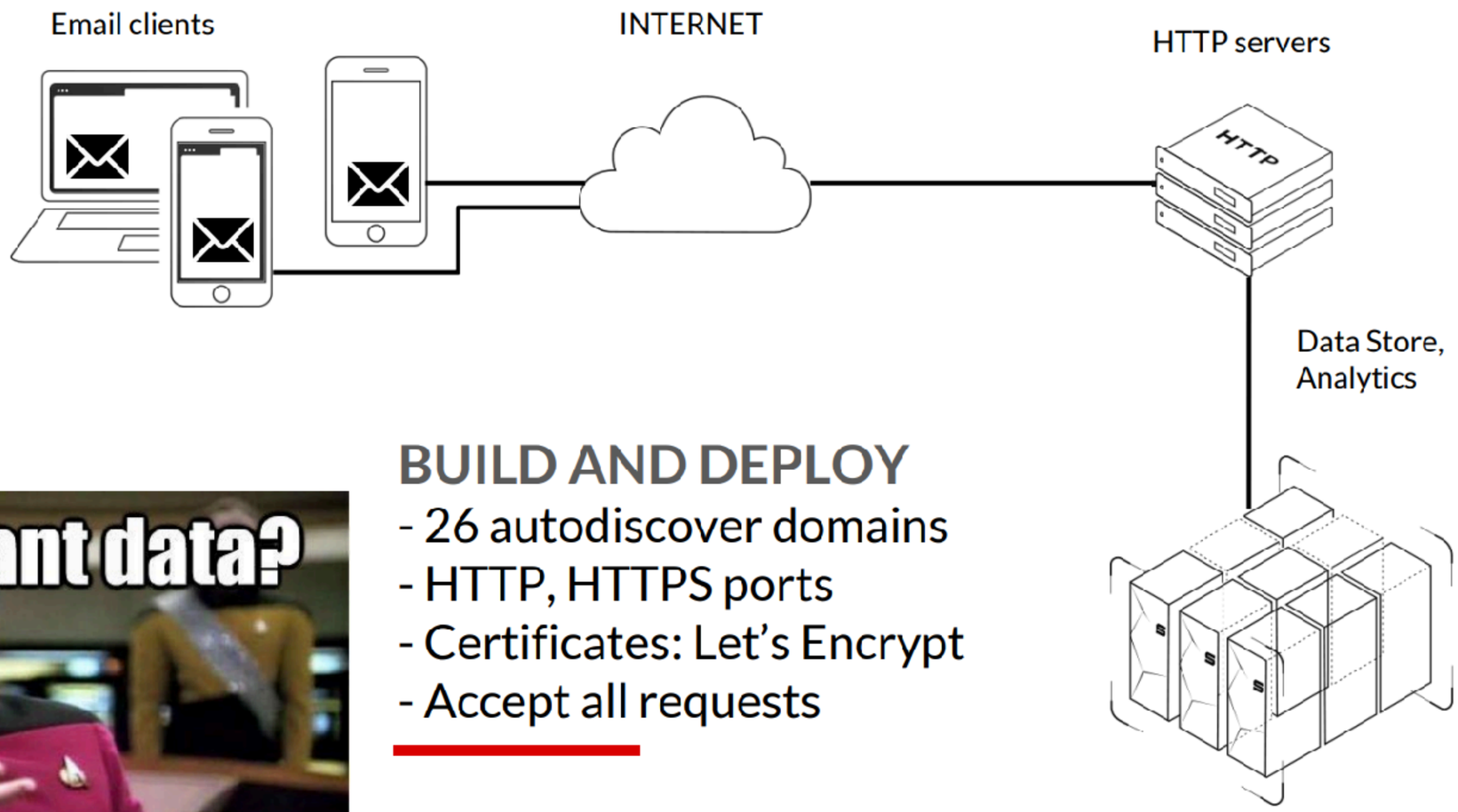


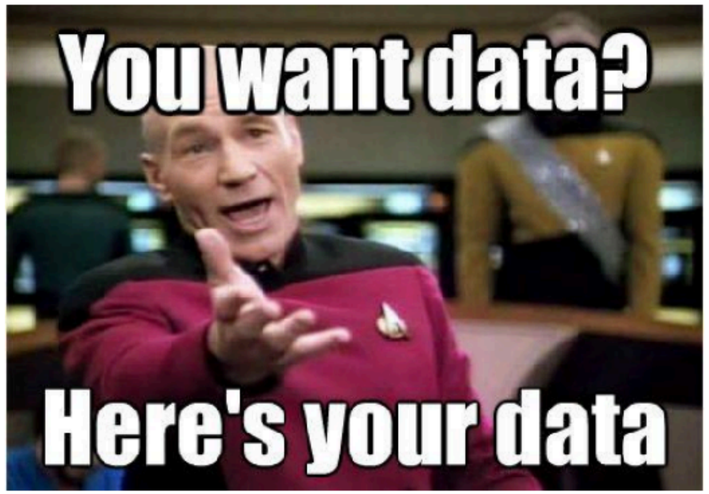
autodiscover. + <domain>

autodiscover.com

Announced as fixed: March 2017. iOS 10.3

AUTODISCOVER : TECH

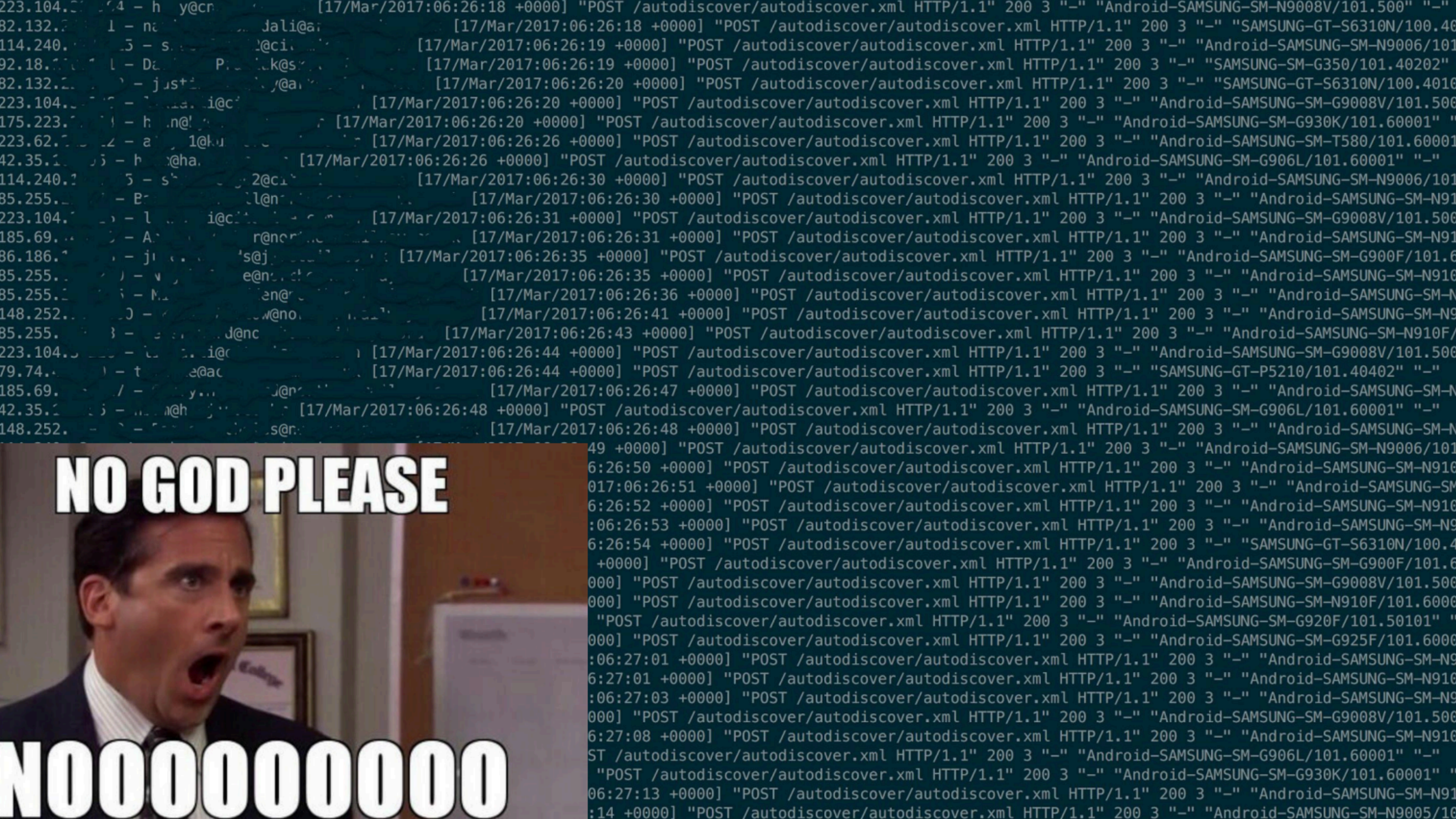




BUILD AND DEPLOY

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

* It's just a simple HTTP sink


NO GOD PLEASE
NOOOOOOOOO

PASSIVE ATTACK RESULTS

22M

REQUESTS RECEIVED

18M

REQUESTS WITH BASIC AUTHENTICATION HEADERS

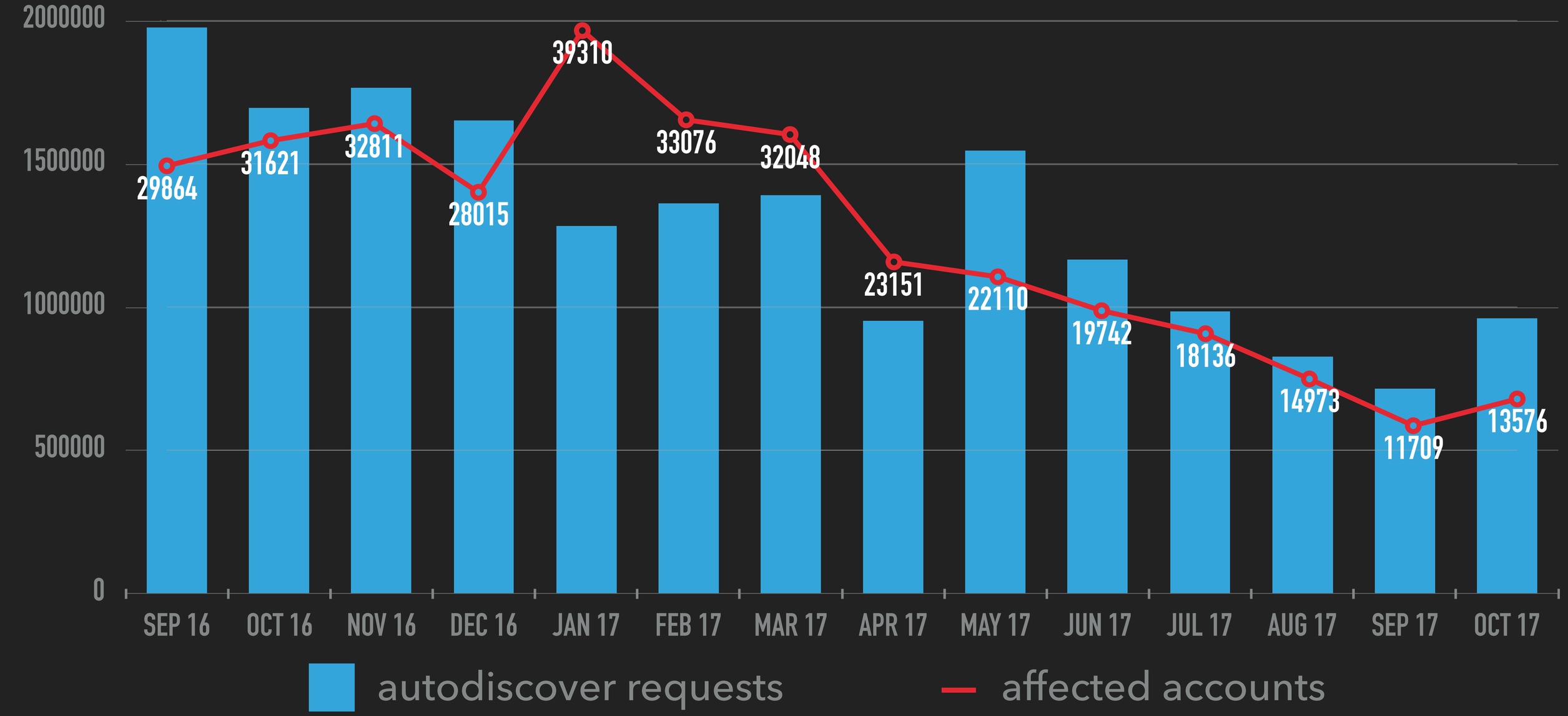
353K

EMAIL ACCOUNTS AFFECTED

we need to come up with a better name

SEPTEMBER 16 TO OCTOBER 17

TRENDS


2000000
1500000
1000000
500000
0
29864
31621
32811
28015
39310
33076
32048
23151
22110
19742
18136
14973
11709
13576
SEP 16
OCT 16
NOV 16
DEC 16
JAN 17
FEB 17
MAR 17
APR 17
MAY 17
JUN 17
JUL 17
AUG 17
SEP 17
OCT 17
autodiscover requests
affected accounts

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

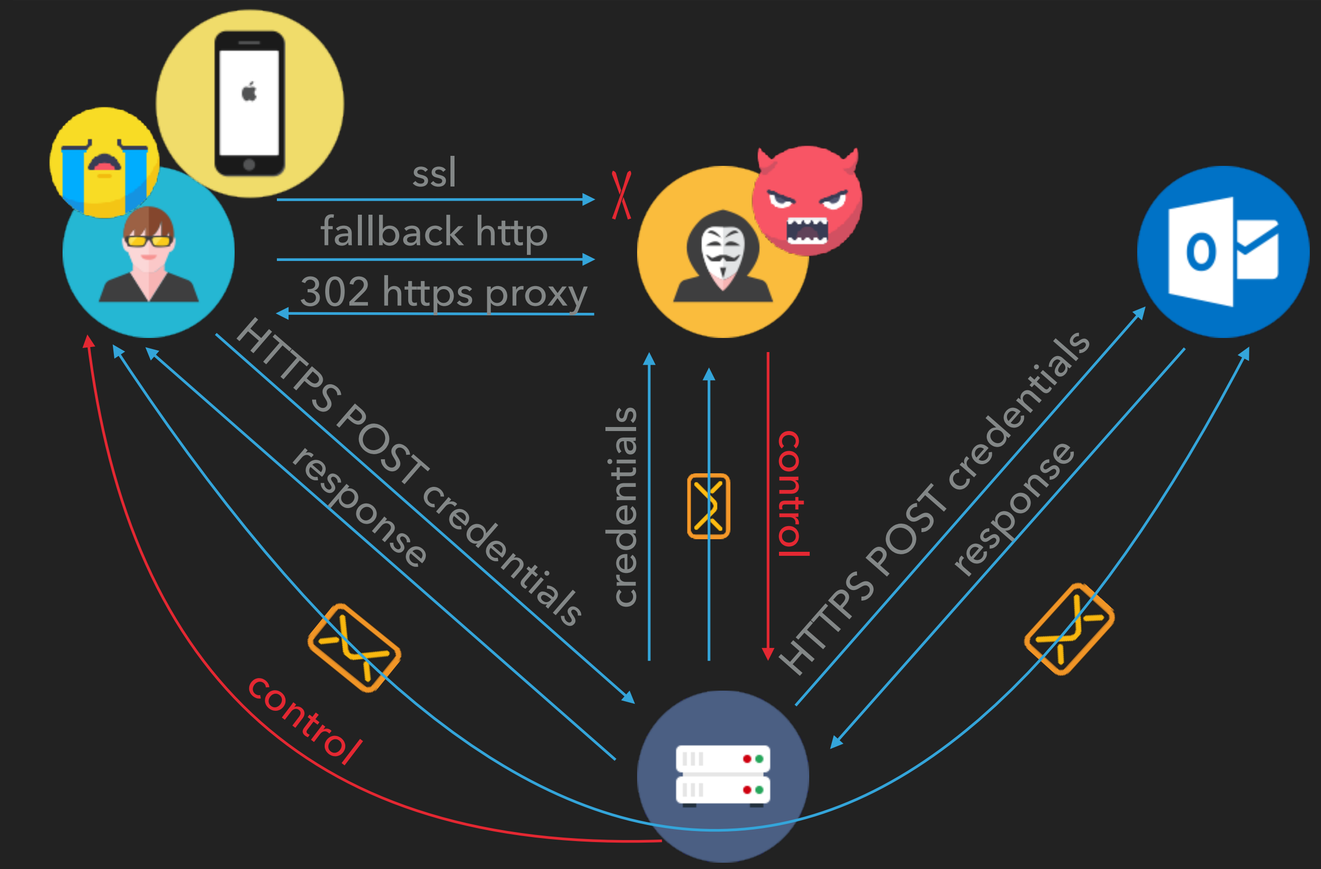
CLIENT REFRESH CONFIGURATION PERIODICALLY

FALLBACK TO INSECURE PROTOCOLS:

- GET REQUEST TO HTTP
- DNS QUERY

LET'S MITM!

NOW WHAT?


ssl
fallback http
302 https proxy
HTTPS POST credentials
response
credentials
control
HTTPS POST credentials
response
control

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

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 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

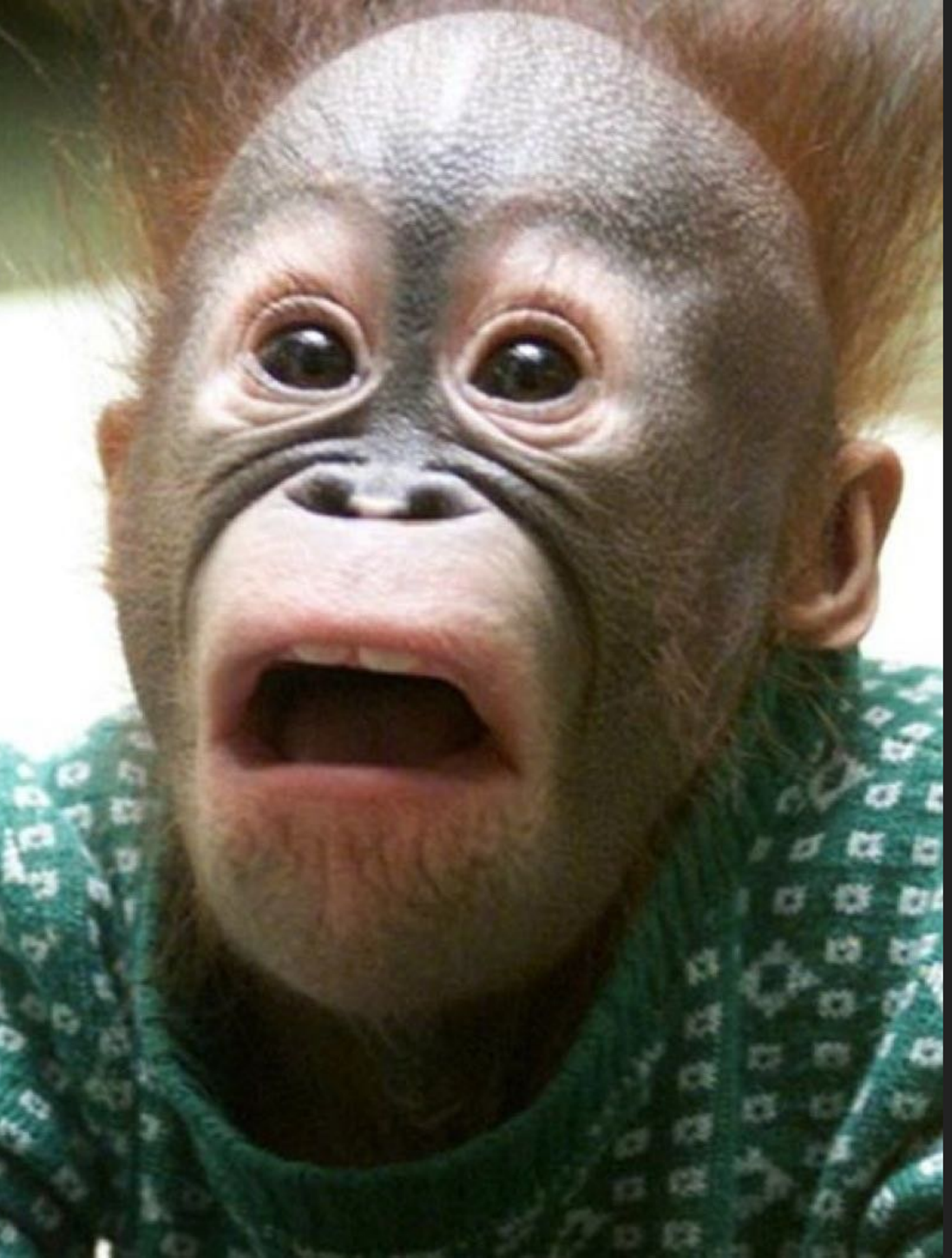
PUBLISHED: 08:21, Fri, Sep 22, 2017 | UPDATED: 08:21, Fri, Sep 22, 2017

DEMO TIME

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?

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