

ALL YOUR EMAILS BELONG TO US

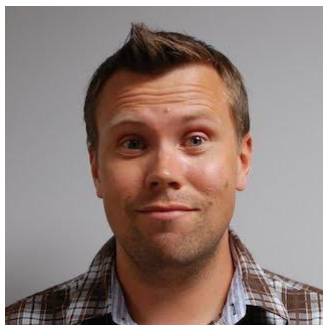
Exploiting vulnerable email clients via domain name collision

March 2017

Ilya Nesterov, Max Goncharov

Who we are

Ilya Nesterov



I break things
I build things to break things
Security researcher
Shape Security

Max Goncharov



Security researcher
Threat OSINT
Vuln. hunter
Shape Security

Email? What is wrong with that?



Email? What is wrong with that?

A photograph of three men and a baby on a staircase. The man on the left has a beard and sunglasses, wearing a grey t-shirt and carrying a baby in a black carrier. The man in the middle has a beard and is wearing a light blue button-down shirt. The man on the right is wearing glasses and a light blue polo shirt, with his arm raised. The background is a yellow wall with a staircase railing.

AUTODISCOVER

Autodiscover : History

2006



2008



2009



2010



2017

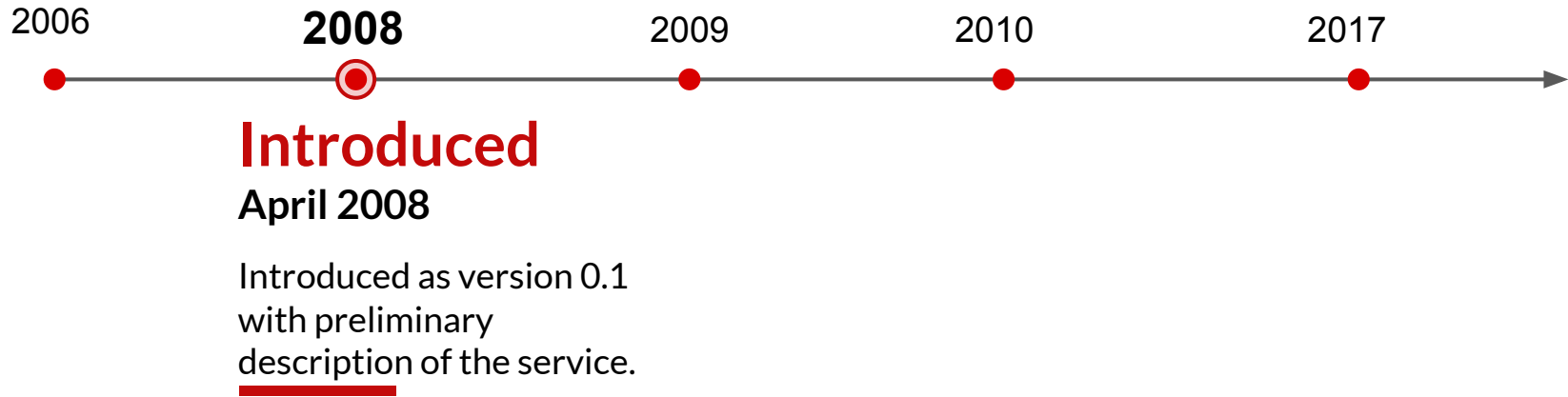


Feature

for Office 2007

Autodiscover announced
as a feature for the
upcoming product release

Autodiscover : History



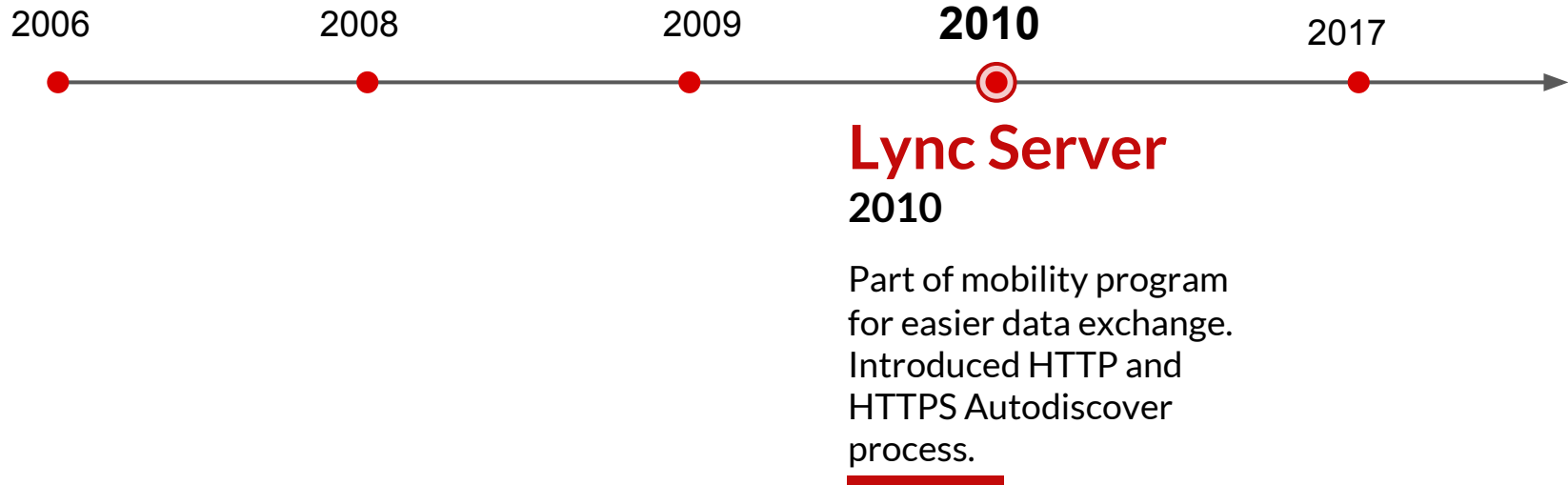
Autodiscover : History



Thunderbird config-v1.1.xml

Alternative of Autodiscover for
Thunderbird proposed in 2008
and released in 2009.

Autodiscover : History



Autodiscover : History

2006

2008

2009

2010

2017



**Here we are
With Autodiscover**

We found severe vulnerabilities in some autodiscover client implementations.

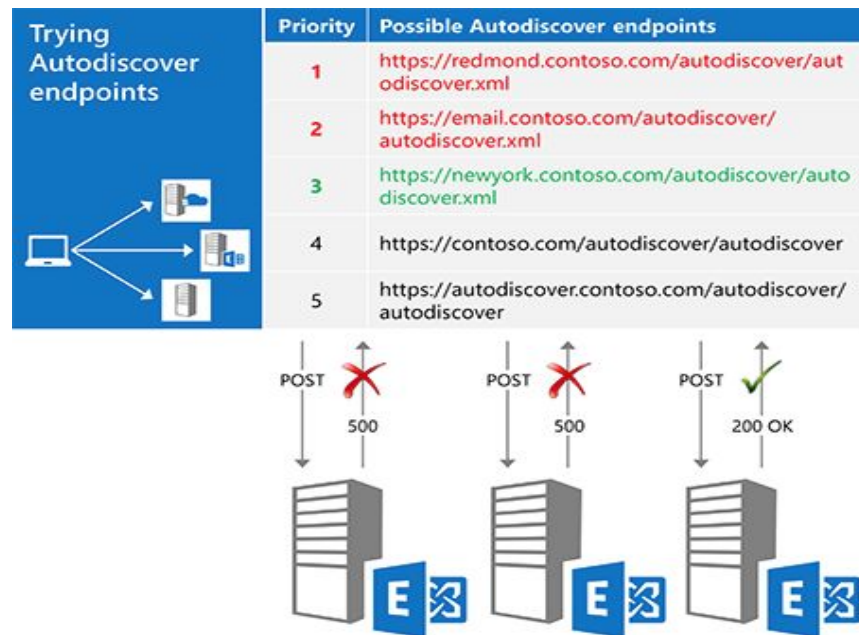
Autodiscover : Process

1. Define the candidate pool
2. Try each server from a list



Defining the candidate pool

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. Prioritize



Derive URL from the email

tomknopf77@jarzt.com



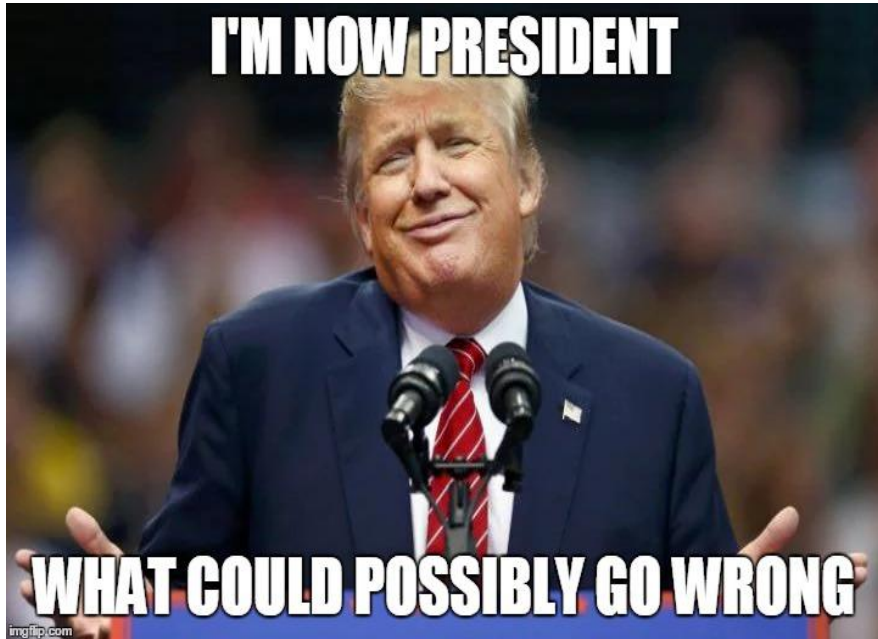
jarzt.com

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`

What can be wrong?



local@domain

tomknopf77@jarzt.com



Local: tomknopf77

Domain: jarzt.com

Email address complexity

RFC 5321

RFC 5322

RFC 6531

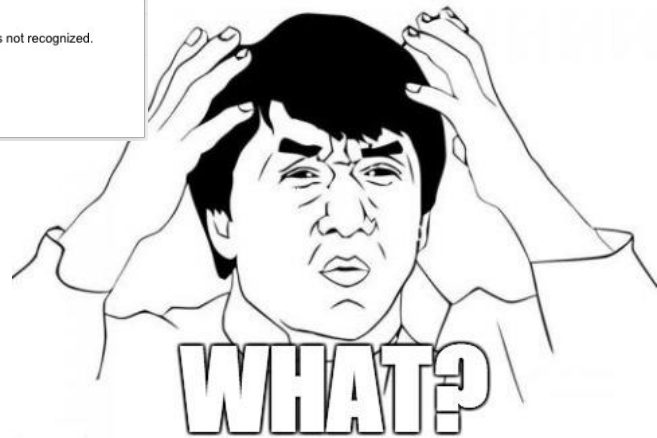
RFC 6532

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

✗ tom@knopf77@jarzt.com



✓ "tom@knopf77"@jarzt.com



Samsung Mail Client

CVE-2016-9940



tomknopf77@example.com.au



autodiscover.example.com.au

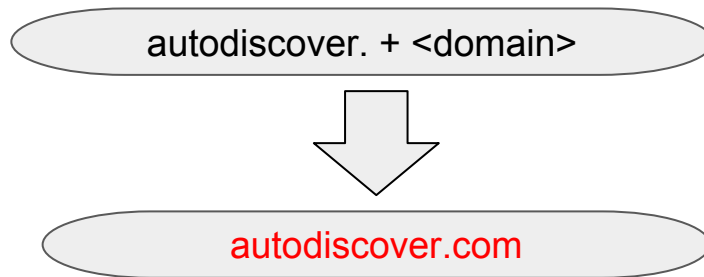
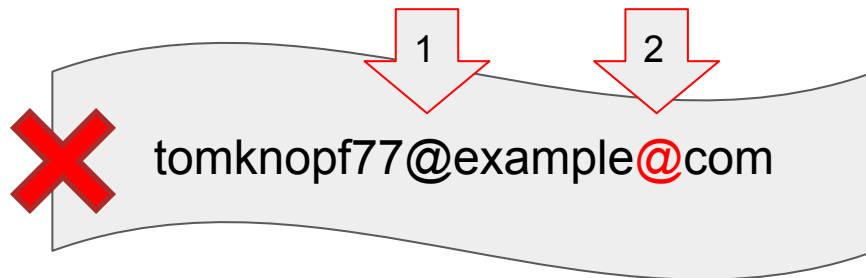


autodiscover.com.au

Announced as fixed: January 2017

iOS Mail app

CVE-2017-2414



Announced as fixed: March 2017. iOS 10.3

We need more data!

8K+

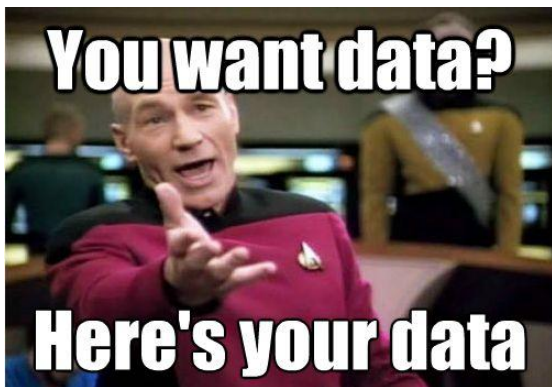
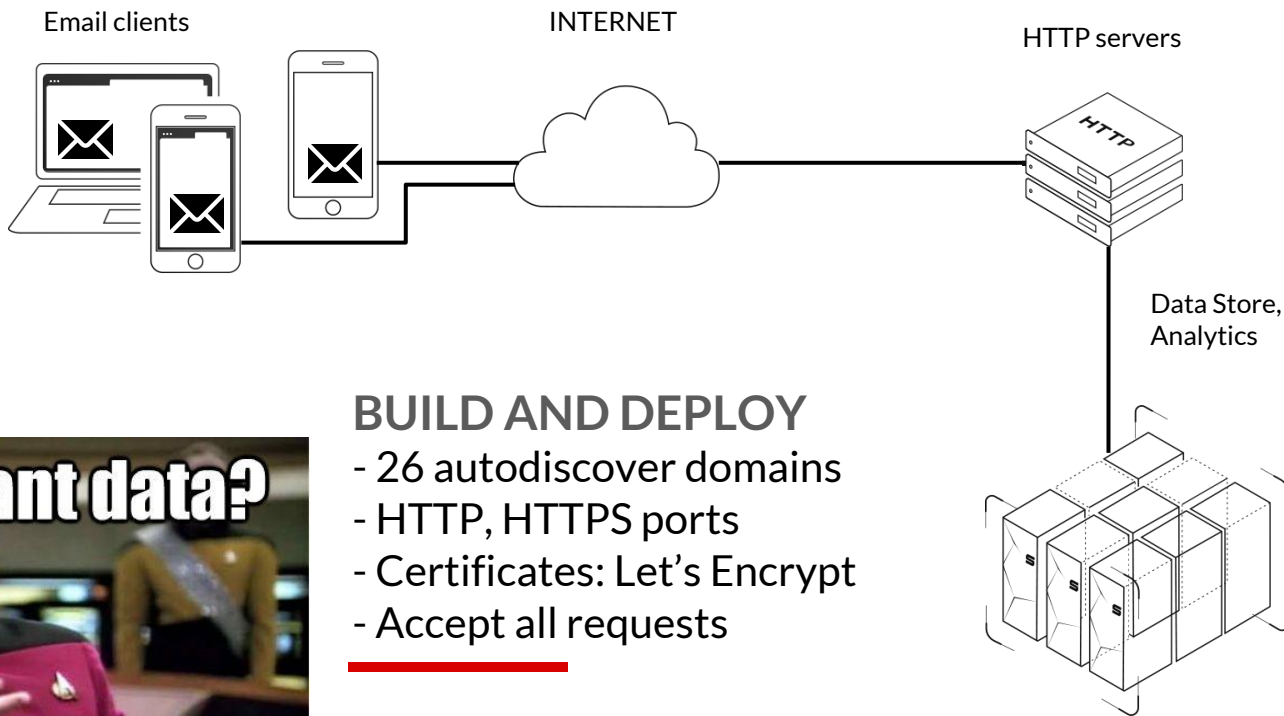
Mozilla public suffix list

1.5K+

IANA TLD list



Let's build a hacking machine!*



* It's just a simple HTTP sink

Logs! This is ... scary!

```
223.104.201.104 - h_y@cn [17/Mar/2017:06:26:18 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9008V/101.500" "-"
82.132.7.1 - na [17/Mar/2017:06:26:18 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-GT-S6310N/100.40102" "-"
114.240.1.5 - s [17/Mar/2017:06:26:19 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9006/101.500" "-"
92.18.1.1 - Da [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 [17/Mar/2017:06:26:20 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-GT-S6310N/100.40102" "-"
223.104.201.104 - h_y@cn [17/Mar/2017:06:26:20 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9008V/101.500" "-"
175.223.7.1 - h_y@cn [17/Mar/2017:06:26:20 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G930K/101.60001" "-"
223.62.7.1 - a [17/Mar/2017:06:26:26 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-T580/101.60001" "-"
42.35.1.1 - h_y@ha [17/Mar/2017:06:26:26 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G906L/101.60001" "-"
114.240.1.5 - s [17/Mar/2017:06:26:30 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9006/101.500" "-"
85.255.1.1 - B [17/Mar/2017:06:26:30 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
223.104.201.104 - h_y@cn [17/Mar/2017:06:26:31 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G9008V/101.500" "-"
185.69.1.1 - A [17/Mar/2017:06:26:31 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
86.186.1.1 - j [17/Mar/2017:06:26:35 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G900F/101.60001" "-"
85.255.1.1 - e [17/Mar/2017:06:26:35 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
85.255.1.1 - M [17/Mar/2017:06:26:36 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
148.252.1.1 - J [17/Mar/2017:06:26:41 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
85.255.1.1 - J [17/Mar/2017:06:26:43 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
223.104.201.104 - h_y@cn [17/Mar/2017:06:26:44 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G9008V/101.500" "-"
79.74.1.1 - t [17/Mar/2017:06:26:44 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-GT-P5210/101.40402" "-"
185.69.1.1 - y [17/Mar/2017:06:26:47 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
42.35.1.1 - h_y@ha [17/Mar/2017:06:26:48 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-G906L/101.60001" "-"
148.252.1.1 - J [17/Mar/2017:06:26:48 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
49 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9006/101.500" "-"
6:26:50 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
017:06:26:51 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
6:26:52 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
:06:26:53 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
6:26:54 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "SAMSUNG-GT-S6310N/100.40102" "-"
+0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N900F/101.60001" "-"
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/101.60001" "-"
"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/101.60001" "-"
:06:27:01 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
6:27:01 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
:06:27:03 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N910F/101.60001" "-"
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-N910F/101.60001" "-"
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-N910F/101.60001" "-"
:14 +0000] "POST /autodiscover/autodiscover.xml HTTP/1.1" 200 3 "-" "Android-SAMSUNG-SM-N9005/101.500" "-"
```

NO GOD PLEASE

NOOOOOOOOO

RESULTS

7

Month period
Sep 2016 - March 2017

26

Domains in experiment

13M

Total requests received

9M

Requests with Basic
Authentication header

2473

Different Autodiscover
client user-agents

212K

Email accounts affected from
65K different domains

MITIGATION

Users:

- use recommended email clients
- install security updates

Enterprise:

- follow official deployment guides
- use only supported email clients
- test all third party clients
- check your deployment regularly

Developers:

- follow Autodiscover specification
- derive local and domain parts properly
- remember TLD and public suffix list
- test, test, test

ICANN:

- ban autodiscover domain registration

Conclusion

EMAIL IS COMPLICATED

It is even more complicated than you think!

READ THE DOCS!

Even if you read it. Read between the lines

NOBODY IS PERFECT

We all make mistakes. Let's learn from someone else's experience

Demo!

Thank You