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?

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.

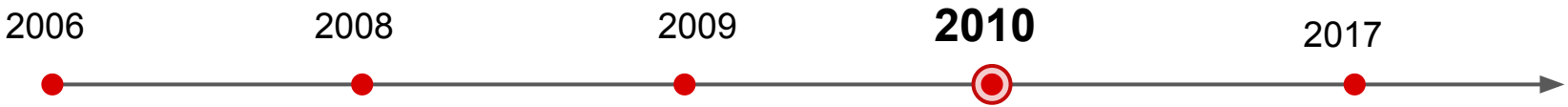
Autodiscover : History

Thunderbird

config-v1.1.xml

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

Autodiscover : History



Lync Server

2010

Part of mobility program for easier data exchange. Introduced HTTP and HTTPS Autodiscover process.

Autodiscover : History

2006 — 2008 — 2009 — 2010 — **2017**

Here we are

With Autodiscover

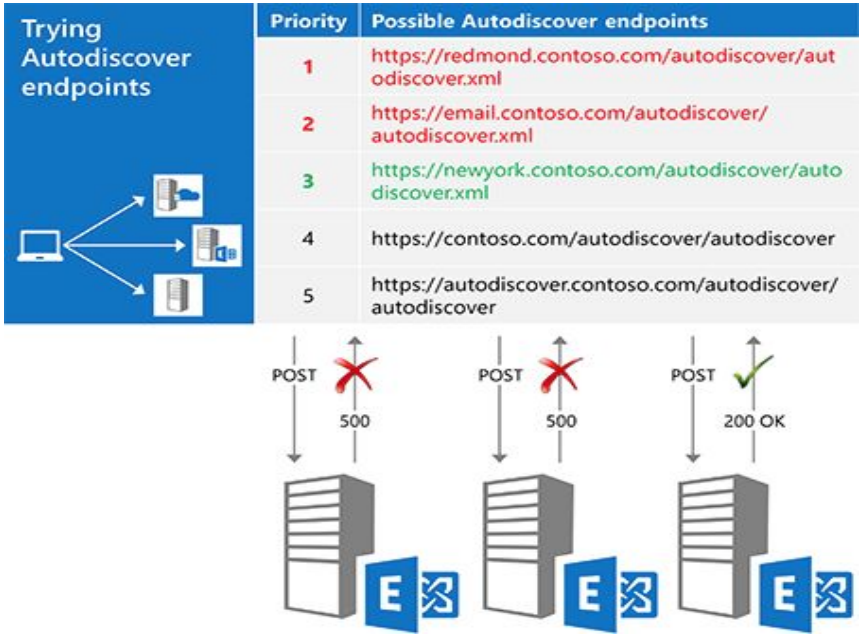
We found severe vulnerabilities in some autodiscover client implementations.

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

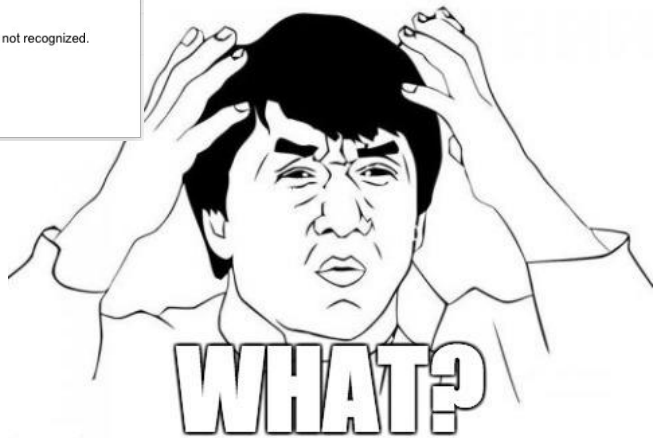
RFC 6531

RFC 6532

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

✗ tom@knopf77@jarzt.com

✓ "tom@knopf77"@jarzt.com



Samsung Mail Client

CVE-2016-9940

tomknopf77@example.com.au

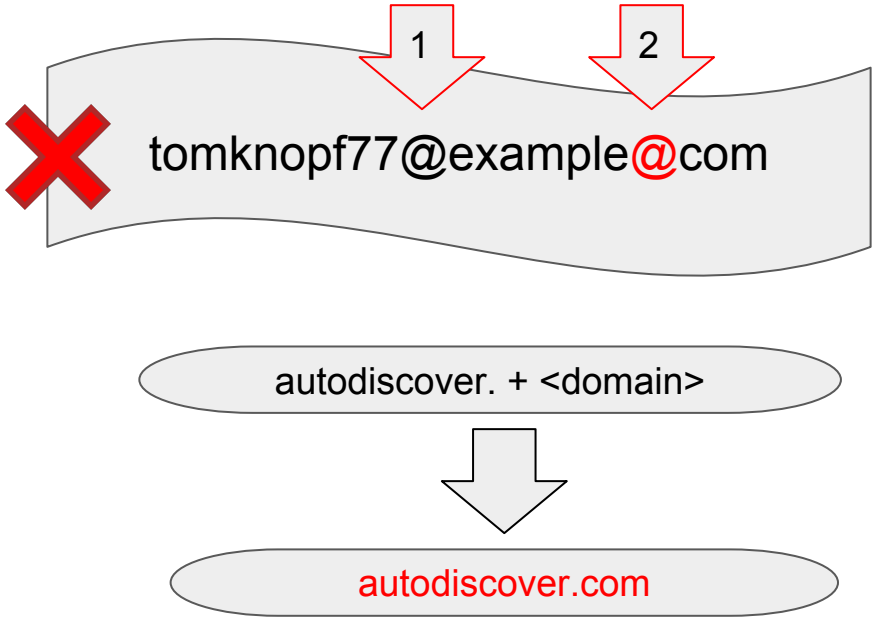
✓ autodiscover.example.com.au

✗ 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!

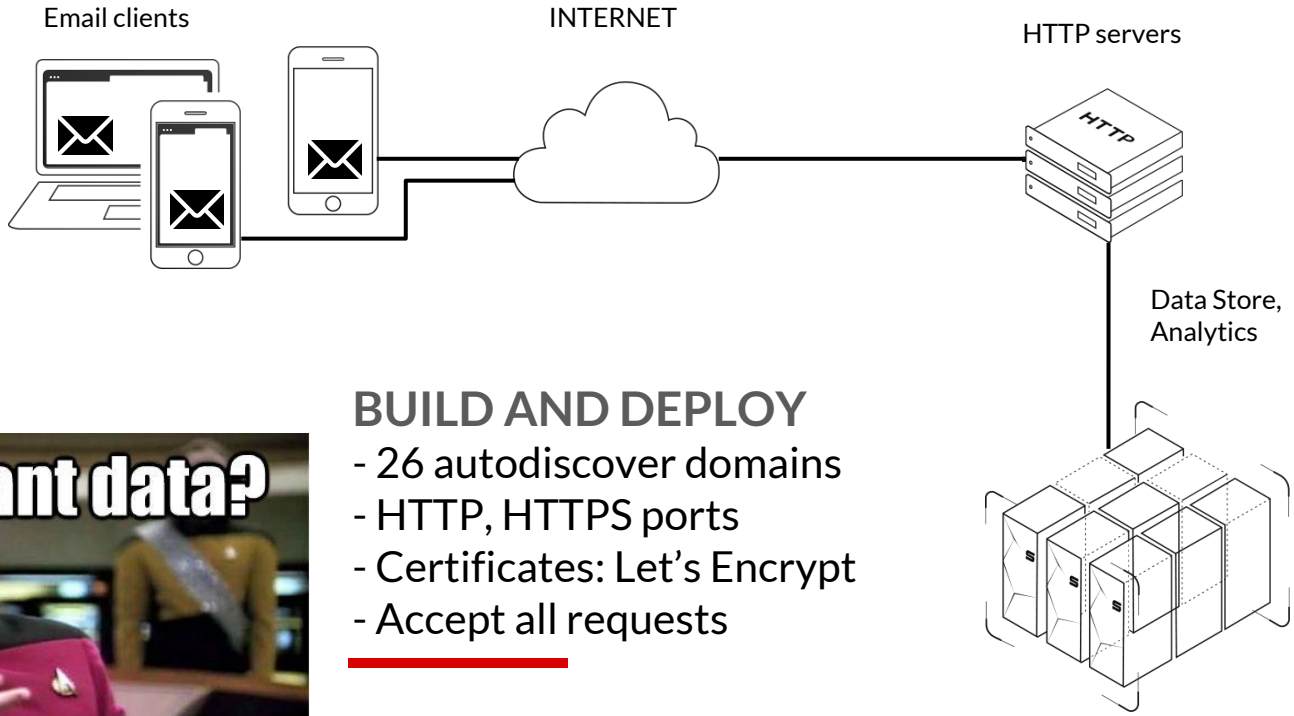
8K+

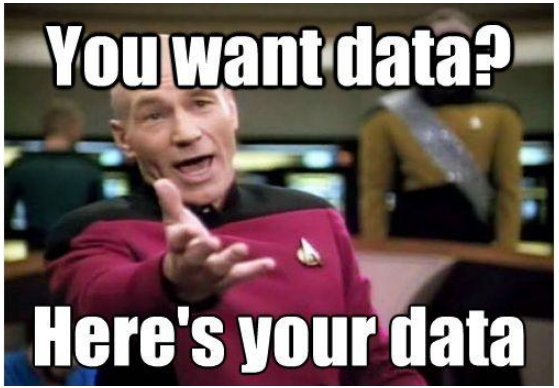
Mozilla public suffix list

1.5K+

IANA TLD list

Let’s build a hacking machine!*



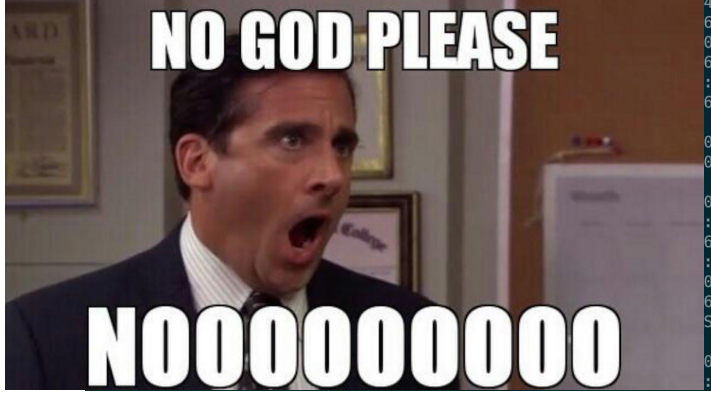


BUILD AND DEPLOY

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

* It’s just a simple HTTP sink

Logs! This is … scary!



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