OH MY H@CK 2021

Autodiscover -> Autodisclose

Link do prezentacji:

https://github.com/sq5bpf/misc/blob/master/omh2021.pdf

Jacek Lipkowski SQ5BPF

~$ whoami

- Jacek Lipkowski SQ5BPF@lipkowski.org
- Hobby:
- Krótkofalarstwo. Znak SQ5BPF
- (od ponad 25 lat, licencja z roku 1993)
- Unixy, sieci. I ich psucie :) (od 25 lat)
- Elektronika (od zawsze)

- Pracuje w Pekao Financial Services Sp. z o.o.
- Prezentacja ta jest moja i nie wyraża poglądów pracodawcy.

O czym jest ta prezentacja?

- Pasmo porażek
- Pierwsza porażka: Temat mi nie wypalił (miało być o radiu oczywiście :)
- Znalazłem jakieś dziwne zapytania DNS, poszukałem od czego one są.
- Co to jest Exchange Autodiscover Service
- Loginy/hasła spadają z nieba
- Aktywne ataki

Dziwne zapytania DNS

Dużo zapytań o autodiscover.JEDNA_Z_MOICH_DOMEN w logach DNS:

15-Feb-2021 15:46:33.627 info: client 213.158.204.XXX#15435 (autodiscover.JEDNA_Z_MOICH_DOMEN): query: autodiscover.JEDNA_Z_MOICH_DOMEN IN A -E (X.X.X.X)

I na serwerze WWW:

62.251.100.XX - - [15/Sep/2021:15:56:04 +0200] "GET /autodiscover/autodiscover.xml HTTP/1.1" 302 321 "-" "Microsoft Office/16.0 (Microsoft Outlook Mail 16.0.6308; Pro)"

37.225.17.XX - - [16/Oct/2021:19:45:12 +0200] "GET /autodiscover/autodiscover.xml HTTP/1.1" 302 358 "-" "Android-SAMSUNG-SM-A202F/101.11"

Autodiscover for Exchange

https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/autodiscover-for-exchange

Protokół autokonfiguracji klienta pocztowego do Exchange.

Konfigurujemy konto: USER@DOMENA_MAILA

Fazy 1 i 2:

- SCP (service control point) endpoint z AD
- https://DOMENA_MAILA/autodiscover/autodiscover.xml
- https://autodiscover.DOMENA_MAILA/autodiscover/autodiscover.xml

Musi być HTTPS i musi być prawidłowy certyfikat.

Faza 3:

- http://autodiscover.DOMENA_MAILA/autodiscover/autodiscover.xml (redirect 302 do https)
- Rekord SRV _autodiscover._tcp.DOMENA_MAILA

Porażka: odłożone na później

A może coś a’la badWPAD ?

Automatyczna konfiguracja proxy w IE ściągana jest z http://wpad/wpad.dat

DNS devolution: resolver odcina kolejne człony domeny aż nazwa się rozwiąże (ktoś kiedyś stwierdził że to świetny pomysł i tak zostało).

workgroup.domena.com.pl:

- wpad.workgroup.domena.com.pl
- wpad.domena.com.pl
- wpad.com.pl :)

  Może zadziała też z autodiscover? :)
- 4 sierpnia 2021 zarerejstrowałem autodiscover.com.pl

  (i net.pl, org.pl, edu.pl :). Wtedy mógłbym zarejestrować więcej :)

  Lista suffiksów domen: https://publicsuffix.org/

autodiscover.com.pl

Na porcie 443: certyfikat z Let’s Encrypt.

Dla /autodiscover/* loguje nagłówek i zwracam 404.

Na porcie 80: 301 albo 302 redirect z /URI do https://autodiscover.com.pl/URI

autodiscover.com.pl

Porażka: to tak nie działa jak BadWPAD.

Ale i tak jest fajnie :) Zarejestrowałem tylko jedną domenę i caly internet wysyła mi setki loginów/haseł, bez jakiegokolwiek działania z mojej strony.

Authorization: Basic cGllcndzemVtdS5rdG8uZG8ubW5pZS5uYXBpc3plOnN0YXdpYW0ucGl3bw==

MS-ASProtocolVersion: 2.5

Connection: keep-alive

User-Agent: SAMSUNG-GT-I9305/101.40404

Content-Type: text/xml

Accept: text/xml, text/html

Content-Length: 378

Host: autodiscover.com.pl

Porażka, było poszukać w internecie:

„All your emails belong to us: exploiting vulnerable email clients via domain name collision”

Ilya Nesterov, Maxim Goncharov. BlackHat Asia 2017

https://www.blackhat.com/docs/asia-17/materials/asia-17-Nesterov-All-Your-Emails-Belong-To-Us-Exploiting-Vulnerable-Email-Clients-Via-Domain-Name-Collision-wp.pdf

„How Three Low-Risk Vulnerabilities Become One High”

Keiron Shepherd, Raymond Pompon. F5 labs

https://www.f5.com/labs/articles/threat-intelligence/how-three-low-risk-vulnerabilities-become-one-high-24995

Ale to jest z 2016-2018 a hasła nadal spadają z nieba w 2021 :)

autodiscover.com.pl

Co przychodzi (po IP i User-Agent):

- 14205 User-agent: .*SAMSUNG.*
- 4301 sieć 185.XX.YY.0/23 User-agent: Mozilla/4.0 ([...] Microsoft Outlook 15.0.4481; ms-office; MSOffice 15)
- 309 User-agent: .*Android-Mail.* (bez SAMSUNG)
- i dużo innych :)

Główne przyczyny

Klient wpisał adres @com.pl, @net.pl, @edu.pl. @org.pl itp. :

- pomyłki np. biuro.firma@com.pl zamiast biuro@firma.com.pl
- pomyłki user@net.pl zamiast user@onet.pl
- pomyłki łatwy_do_znalezienia_w_google@com.pl
- sporo smieci typu ziom@com.pl:1111

Program pocztowy używa domain devolution (pełna nazwa domeny zamiast np com.pl), głównie stare wersje aplikacji mailowej SAMSUNG-a. Czasem adresy z domen dużych firm (BYOD :).

Unikalne pary login:hasło

- autodiscover.com.pl 1164
- autodiscover.net.pl 137
- autodiscover.org.pl 35
- autodiscover.edu.pl 35

Okres ok 2.5 miesiąca: 6 sierpnia 2021 – 22 października 2021

Skrypty po stronie serwera

klient: GET/POST http://autodiscover.com.pl/autodiscover/autodiscover.xml

serwer: 302 redirect na https://autodiscover.com.pl/autodiscover/autodiscover.xml

klient: POST https://autodiscover.com.pl/autodiscover/autodiscover.xml

serwer: jeśli jest Authorization: Basic to 404, jeśli nie ma to 401 (zaloguj się)

Zwracam 404 ponieważ nie chcę atakować klienta pocztowego.

W nagłówku HTTP są namiary na mnie zakodowane base64.

Aplikacja Gmail na Androida

Zgłoszone 8 sierpnia 2021

- Issue 195879724 (adresy USER@com.pl itp.)

  status: intended behaviour

  Zgadzam się (ale wyciekają hasła).

Firma X

Firma X robi aplikację do poczty, gdzie obróbka tej poczty jest robiona na ich serwerach.

Połączenia są z ich infrastruktury (185.XX.YY.0/23).

Potraktowali poważnie zgłoszenie że adresy typu user@com.pl nie powinny być akceptowane przez ich aplikację. Nie tłumaczyli się że tylko implementują specyfikacje Microsoftu. I przyznali bug bounty :)

Porażka: niestety zgłosiłem późno, więc nie mogę podać nazwy firmy i aplikacji (podam po tym jak potwierdzą że naprawili).

A może aktywny atak? :)

Aktywny atak

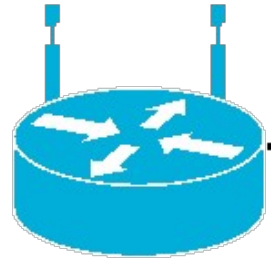
Wifi kontrolowane przez atakującego:

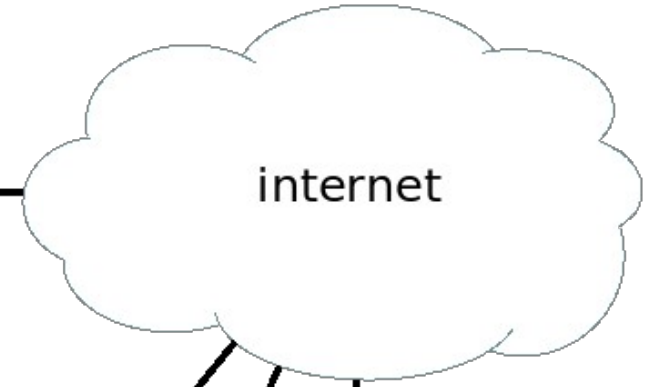
- Wszystkie zapytania DNS kieruje do serwera DNS atakującego
- Puszcza ruch na 80/tcp do IP1 który serwuje redirect
- Puszcza ruch na 443/tcp do IP2 (albo IP1) który serwuje autodiscover.xml
- Blokuje niektóre rodzaje ruchu np DoH i inne (sekret żeby wyszedł atak na niektóre aplikacje) *

DNS kontrolowany przez atakującego:

- rozwiązuje autodiscover.* na IP1
- Blokuje rozwiązywanie niektórych nazw (sekret żeby wyszedł atak na niektóre aplikacje) *

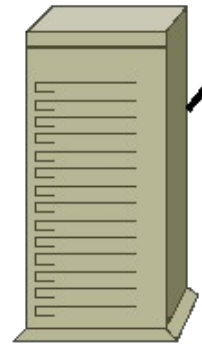
* niestety nadal jest na to embargo

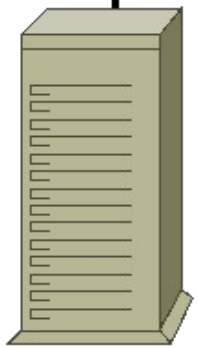




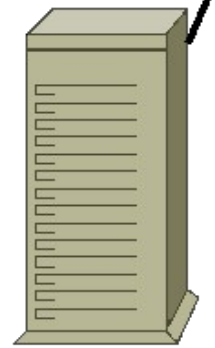
Atakujący:
DHCP
redirect 53/udp do DNS1
80/tcp do IP 1
443/tcp do IP 2

IP 1:
http://XXXX/autodiscover/autodiscover.xml





IP 2:
https://YYYY/autodiscover/autodiscover.xml



DNS1
atakującego
resolvuje
autodiscover.*
na IP 1

DEMO
Aplikacja Gmail
Android

Aplikacja Gmail na Androida

Zgłoszone 9 sierpnia 2021

Issue 195983810 (MiTM, można poznać hasło i podstawić swój autodiscover.xml)

„I believe this one is working as intended.”

„I still think this is an Microsoft problem as its down to how they're requiring Autodiscover to work. If the autodiscover protocol requires fallback to an unsafe standard and the client is required to implement it, the problem is in the standard, not the client that's implementing it. [...]

I think this probably needs to be reported to Microsoft as a problem within autodiscover as a protocol rather than individual clients potentially breaking the implementation by stopping a connection vector.”

Zgadzam się (ale można spowodować wyciek haseł).

Przynajmniej nie ma embargo i mogę pokazać demo :)

Inna aplikacja na Android*

Błędy w zasadzie analogiczne do aplikacji Gmail.

Różni się tym co trzeba puścić/zablokować żeby zrobić atak (można zrobić uniwersalny dla wszystkich przypadków).

Różni się tym że producent aplikacji potraktował temat poważnie.

Nie będzie DEMO*

Producent w 20211105 wydał poprawioną wersję.

* Porażka: znowu embargo

Problemy z autodiscover:

- bugi w starych klientach (załatane, ale nadal wykorzystywane)
- wysyłanie hasła jeśli użytkownik wpisze adres@XXX, gdzie XXX to domena w której możemy kupić autodiscover.XXX
- MiTM, w tym możliwość podłożenia swojego autodiscover.xml

Wzmacniane przez:

- BYOD (Bring Your Own Disaster)
- Praca zdalna (więcej w dobie pandemii)

A może by tak zgłosić do Microsoftu?

Zanim w końcu zainstalowałem windowsy trochę minęło :)

MiTM zgłoszone dopiero 14 września 2021.

Porażka: nadal jest embargo

Publikacja Guardicore

22 albo 23 września Guardicore opublikował: „Autodiscovering the Great Leak”

https://www.guardicore.com/labs/autodiscovering-the-great-leak/

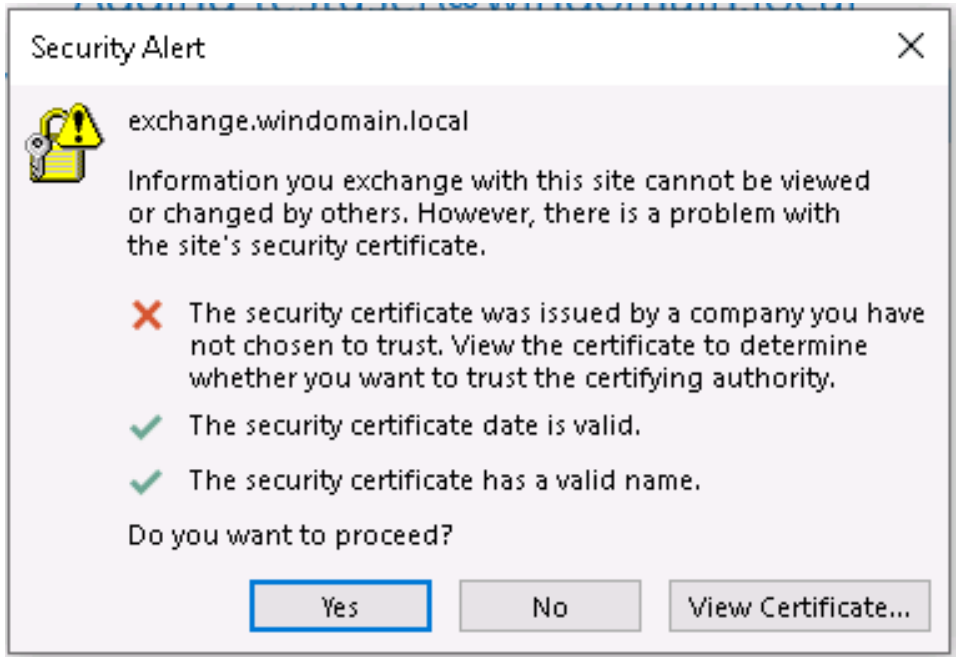
Podobno nie zgłaszali tego Microsoftowi, tylko od razu opublikowali.

Zarejestrowali parę domen autodiscover.* , 97k haseł przez 4 miesiące (u mnie 1371 haseł z 4 domen przez 2 miesiące).

Zrobili atak (MiTM?) „the ol’ switcheroo”. Brak opisu niestety.

Porażka: mogłem wcześniej się zająć tematem i wcześniej zgłosić i opublikować.

Aplikacje Microsoft



Atak Guardicore „The ol' switcheroo"

Błąd certyfikatu, ale i tak opcją domyślną jest „Yes" :)

Ze względu na embargo nie pokażę demo bez czerwonego krzyżyka. Ale przynajmniej dzięki Guaricore mogę pokazać cokolwiek.

Podsumowanie

Porażka: było się tym wcześniej zainteresować.

Porażka: nie mogę wszystkiego pokazać ze względu na embargo.

Porażka (nie moja): zgłaszane w 2016 i później. Może trzeba było właśnie zgłoszenia Guardicore ktoś to ruszył.

Nie porażka (w końcu!): dziś (22 października 2021) w zasadzie już nie dostaje haseł na autodiscover.com.pl. Coś poprawiono :)

Warto czasem spojrzeć krytycznie nawet na „znane” aplikacje.

A co z domenami autodiscover.*.pl ?

Podobno Microsoft rejestruje hurtowo domeny autodiscover.* po publikacji Guardicore.

26 września 2021 zgłosiłem do CERT NASK czy nie chcieliby przejąć domen (tak jak przejeli domeny od badWPAD):

- autodiscover.com.pl
- autodiscover.net.pl
- autodiscover.org.pl
- autodiscover.edu.pl

Brak porażki: Odpowiedź pozytywna

PYTANIA?

VY 73

Jacek Lipkowski SQ5BPF

SQ5BPF@lipkowski.org

Link do prezentacji:

https://github.com/sq5bpf/misc/blob/master/omh2021.pdf